

CRS Report for Congress

Received through the CRS Web

Securing General Aviation

December 15, 2005

Bart Elias
Specialist in Aviation Safety, Security, and Technology
Resources, Science, and Industry Division

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 15 DEC 2005		2. REPORT TYPE		3. DATES COVERED 00-00-2005 to 00-00-2005	
4. TITLE AND SUBTITLE Securing General Aviation				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Congressional Research Service ,The Library of Congress,101 Independence Ave SE,Washington,DC,20540-7500				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 46	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Securing General Aviation

Summary

General aviation (GA) – a catch-all category that includes about 57% of all civilian aviation activity within the United States – encompasses a wide range of airports, aircraft, and flight operations. Because GA plays a small but important role in the U.S. economy, improving upon GA security without unduly impeding air commerce or limiting the freedom of movement by air remains a significant challenge. However, policymakers have received mixed signals about the relative security risk posed by GA, due to its diversity and a general lack of detailed information regarding the threat and vulnerability of various GA operations. While some recent high-profile breaches of GA security point to persisting vulnerabilities and limited intelligence information suggests a continued terrorist interest in using GA aircraft, it is evident that GA airports, aircraft, and operations vary significantly with regard to security risk. While the small size and slow speed of most GA aircraft significantly limits the risk they pose, some experts still fear that they could be used as a platform for a chemical, biological, radiological, or nuclear attack. Certain sectors of GA such as crop dusters and larger business aircraft present more specific risks because of their unique capabilities and aircraft characteristics.

Because various segments of GA differ significantly in terms of their perceived risk, mitigation strategies should arguably be tailored to some degree based on risk. In step with the premise that security measures should be predicated on assessments of risk, a provision in the FY2006 Department of Homeland Security Appropriations Act (P.L. 109-90) requires the DHS to examine the vulnerability of high-risk sites to possible terrorist attacks using GA aircraft. Based on an analysis of risk, a variety of options exist for mitigating security risks that can be tailored to specific GA airports and operations. These include surveillance and monitoring; airport access controls; background checks and vetting of pilots, airport workers, and others having access to GA facilities; and physical protections for airports and aircraft. Steps may also be taken to address unique security risks in agricultural aviation, at flight schools, and among business and charter operators. Besides these steps to enhance GA security at airport and operator sites, homeland security efforts since 9/11 have focused extensively on restricting access to airspace around sensitive locations. These airspace restrictions have been highly contentious because they have a direct impact on the freedom of movement by air, they are costly and resource intensive to implement effectively, and their effectiveness in preventing terrorist attacks in some cases is thought to be questionable.

GA security has remained a topic of considerable interest in the 109th Congress. In addition to the requirement to assess risks posed by GA aircraft called for in P.L. 109-90, both H.R. 2649 and H.R. 3397 propose options to enhance GA security. Addressing lingering concerns over restricted airspace violations in the Washington, DC area that complicate the task of protecting sites from aerial attack, H.R. 3465 calls for increased penalties for violators and mandatory training for pilots. GA user groups have largely opposed these measures, calling instead for a risk-based approach to GA security that they maintain does not unduly impede air commerce or compromise aviation safety. This report will be updated as needed.

Contents

What is General Aviation?	2
General Aviation Flight Operations	2
General Aviation Aircraft Types	4
General Aviation Airports	5
The Economic Impact of General Aviation	6
 The Security Challenge	8
 Security Vulnerabilities	9
 Risk Factors Associated with General Aviation	13
 Possible Options to Mitigate the Security Risks of General Aviation	17
Security Risk Assessments	18
Surveillance and Monitoring	21
Airport Watch Program	22
Behavior Pattern Recognition	23
Airport Access Controls	25
Background Checks and Vetting	27
Physical Security Measures for Airports	30
Physical Security Measures for Aircraft	30
Securing Agricultural Aviation Operations	31
Flight School Security	32
Security Best Practices for Business and Charter Aviation	33
The TSA Access Certificate Program	33
Access to Ronald Reagan Washington National Airport	34
Security Measures for Charter Operations	35
Airspace Restrictions	36
Airspace Restrictions Around Washington, DC	36
Security-Related Flight Restrictions Throughout the United States ..	37
Presidential Airspace Restrictions	37
Policy Issues Regarding Airspace Restrictions	38
Surveillance and Monitoring of Restricted Airspace	38
Airspace Protection and Homeland Defense	39
 Related Legislative Actions in the 109 th Congress	41

List of Figures

Figure 1. The General Aviation Fleet	4
--	---

List of Tables

Table 1. U.S. General Aviation Fleet and Activity	3
---	---

Securing General Aviation

When the term general aviation (GA) is mentioned, the image most likely to be conjured is one of a small single-engine airplane droning over America's farmland on a tranquil summer's day. In the post-9/11 context, this pastoral image of GA has been tarnished to a degree by knowledge that the 9/11 hijackers trained in small general aviation aircraft in the United States and amid lingering concerns that GA aircraft could be used in a future terrorist attack. While some recent high-profile breaches of GA security have pointed to persisting vulnerabilities, and limited intelligence information may suggest a possible terrorist "fixation"¹ on using aircraft to attack U.S. interests, GA aircraft vary significantly with regard to the risks they pose. The threats and vulnerabilities of a small single-engine airplane operating in rural settings is intuitively quite different than the risk characteristics of large business jets operating in and near major metropolitan areas. Most experts agree that an adaptive approach to securing GA aircraft and airports that takes into account the unique risk characteristics of the various distinct components of GA is needed to assure that security needs are adequately met and balanced with economic considerations of the GA industry.²

Policymakers have received mixed signals about the relative risk posed by general aviation. While the 9/11 Commission asserted that "[m]ajor vulnerabilities still exist in ...general aviation security,"³ the commission did not further elaborate on the nature of those vulnerabilities nor did it make specific recommendations pertaining to GA security. The FAA has noted that "[w]hile the DHS has no specific information that terrorist groups are currently planning to use general aviation (GA) aircraft to perpetrate attacks against the United States, it remains concerned that (in light of completed and ongoing security enhancements for commercial aircraft and airports) terrorists may turn to GA as an alternative method for conducting operations."⁴ In other words, while GA aircraft and airports may not be optimally suited for terrorist objectives, the hardening of commercial operations may make them an attractive alternative to terrorists seeking to identify and exploit

¹ See Associated Press. "U.S. Uncovers Al-Qaida Plot in Pakistan; The Terrorist Group Allegedly Planned to Fly an Airplane into the American Consulate." *Telegraph-Herald* (Dubuque, Iowa), May 3, 2003, p. A7.

² See Report of the Aviation Security Advisory Committee Working Group on General Aviation Airport Security (October 1, 2003); and Transportation Security Administration, *Security Guidelines for General Aviation Airports*. Information Publication A-001 (May 2004).

³ National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. New York: W.W. Norton & Co., p. 391.

⁴ Federal Aviation Administration. "Washington, DC Metropolitan Area Special Flight Rules Area; Proposed Rule." *Federal Register*(70) 149 (August 4, 2005), p. 43251.

vulnerabilities in aviation security. In this context, GA airports and aircraft are viewed as comparatively soft targets that may be exploited by terrorists because of known weaknesses and vulnerabilities. This view focuses primarily on the vulnerability of general aviation and does not systematically assess risk with regard to the interaction between these vulnerabilities, the threat posed by GA aircraft, and the potential consequences of a terrorist attack using GA aircraft. In fact, there is considerable debate over the threat element of the risk equation for GA operations. While GA advocates argue that the threat is minimal, some policymakers and security experts have expressed concern that, to the contrary, GA may pose a significant security threat. Part of the difficulty in resolving this debate is the diversity of operations and aircraft types that make up GA, making a single threat assessment for all sectors of the GA industry arguably inappropriate. To put the threat into context, the following discussion provides an overview of the variety of aircraft types, flight operations, and airport characteristics that make up GA. This discussion is followed by an analysis of the existing vulnerabilities in GA security, the terrorist threat posed by GA aircraft, and how these elements factor into a risk-based assessment of GA security. Based on this analysis, possible approaches to GA security are discussed and ongoing initiatives and legislative proposals currently under consideration are reviewed.

What is General Aviation?

In a sense general aviation (GA) is a catch-all phrase that encompasses about 57% of all civil aviation activity within the United States, measured in terms of overall flight hours.⁵ Therefore, it is often easier to frame general aviation in terms of what it is not rather than what it is. In this context, GA refers to most aviation operations not conducted by scheduled passenger airlines, large air cargo operators, or the military. To add to the confusion, commercial charter operations are often grouped in with GA and non-revenue flights, such as maintenance test flights and repositioning flights conducted by passenger and cargo airlines, are usually operated under regulations often regarded as “general aviation” flight rules.⁶ Thus, virtually all flight activity outside the scope of scheduled passenger or cargo air carrier flights and military operations may be considered GA. This encompasses a wide variety of aircraft types and flight operations. **Table 1** shows the distribution of aircraft and flight operations formally categorized as GA.

General Aviation Flight Operations

As indicated in **Table 1**, recreational flying in personal aircraft (personal flying) and flight instruction, the typical activities one might expect to see at a small to mid-

⁵ CRS calculations based on Federal Aviation Administration. *FAA Aerospace Forecasts – Fiscal Years 2005-2016*. March 2005.

⁶ The set of regulations specified in Title 14, Code of Federal Regulations, Part 91 – General Operating and Flight Rules, apply to all civil aircraft operating in the national airspace system. Like GA aircraft, non-revenue airline flights are subject to these rules, but are not subject to additional safety and security regulations specifically applicable to revenue air carrier operations.

sized GA airport, comprises slightly more than half of all GA operations and accounts for about 75% of all aircraft in the total GA fleet. Business and corporate flying – which encompasses anything from small businesses flying cancelled checks or regional salesmen flying to customer sites in small single-engine aircraft, to companies ferrying crews to offshore oil rigs by helicopter, to operations of large corporate jets and professionally managed fractional-ownership fleets – makes up about one-quarter of all GA operations. On-demand charter services, referred to as air taxi services, and air tours are also considered GA operations and make up about 5% of all general aviation operations. In addition to these major categories, there are a wide variety of additional GA operations such as aerial advertising (banner towing and skywriting), aerial application (crop-dusting), aerial photography, mapping and data collection, traffic reporting, air ambulance and medical evacuation, and search and rescue, that account for the remaining 14% of all GA operations.

Table 1. U.S. General Aviation Fleet and Activity

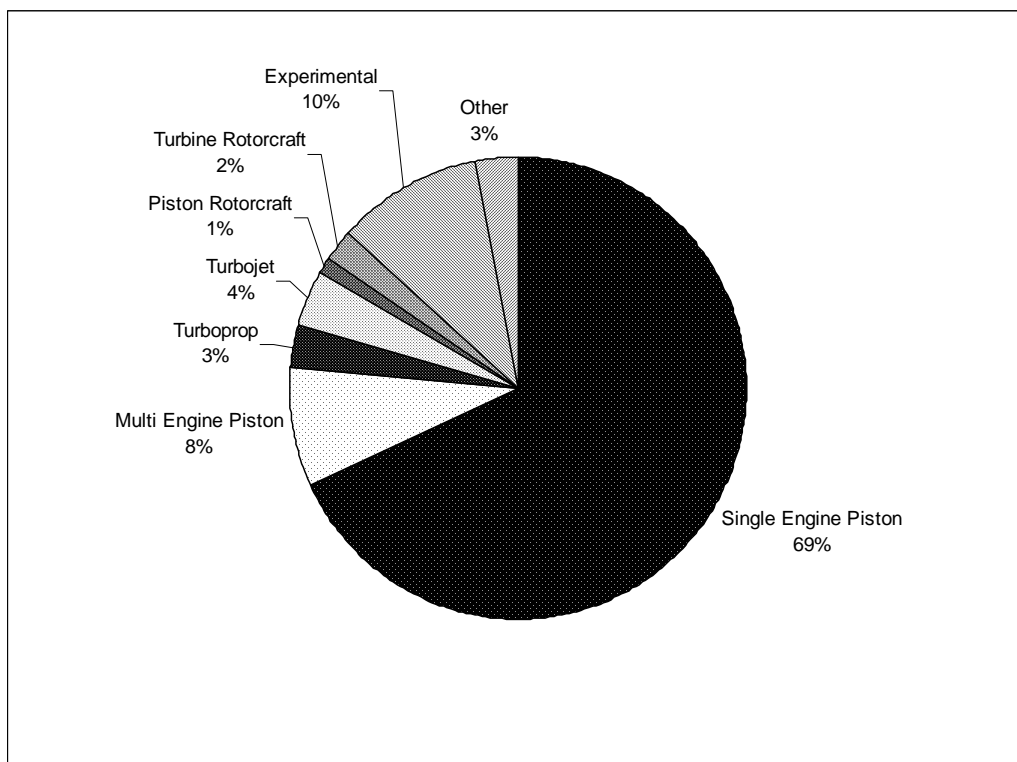
CATEGORY	Number of Aircraft	Percent of GA Fleet	Hours Flown (Millions)	Percent of Operations
Corporate	10,500	5.0	3.2	11.7
Business	25,000	11.9	3.4	12.4
Personal	146,700	70.0	11.3	41.2
Instructional	12,700	6.1	4.4	16.1
Air Taxi/Charter	2,600	1.2	1.2	4.4
Air Tours	200	0.1	0.2	0.7
Aerial Application	3,300	1.6	1.1	4.0
Aerial Observation	4,200	2.0	1.3	4.7
Aerial Other	800	0.4	0.1	0.4
External Load	200	0.1	0.1	0.4
Other Work	1,700	0.8	0.4	1.5
Sightseeing	900	0.4	0.2	0.7
Medical Services	900	0.4	0.5	1.8
TOTAL	209,700	100.0	27.4	100.0

Source: U.S. Department of Transportation, Federal Aviation Administration. *Administrator's Fact Book* (August 2005).

General Aviation Aircraft Types

Because of the diversity of operations considered under the broad definition of general aviation, GA encompasses a wide spectrum of aircraft types. Registered general aviation aircraft in the United States – numbering about 210,000 – range in size and purpose from very light sport aircraft with maximum takeoff weights of less than 1,320 pounds used strictly for recreational flying to very large business jets weighing more than 100,000 pounds used for long-range transcontinental and international travel. The composition of the current GA fleet is shown in **Figure 1**. Single-engine piston aircraft make up the large bulk of the fleet (69%). The large majority of these aircraft are comparably small in size, most weighing less than 5,000 pounds maximum takeoff weight including payload. Experimental aircraft, mostly small home-built airplanes, make up an additional 10% of the current fleet. Thus, while GA is quite diverse, the typical image of a GA aircraft as a small, light, single-engine airplane is an accurate portrayal of the large majority (about 75%) of the GA fleet.

Figure 1. The General Aviation Fleet



Source: Federal Aviation Administration. *FAA Aerospace Forecasts – Fiscal Years 2005-2016*. March 2005.

Although turbojet aircraft are a fast-growing segment of the GA fleet, they comprise only about 4% of the current GA fleet, and this is not expected to change much over the next 10 years. Nonetheless, the growing number of turbojet aircraft has important implications for GA security as these heavier, faster, and more capable aircraft become more and more prevalent. While the numbers of piston aircraft are expected to remain flat and the numbers of GA turboprops are expected to grow only

slightly (about 1.3% annually), the numbers of GA turbojets is forecast to grow at a brisk pace of about 6% per year over the next ten years. By 2016 it is expected that there will be almost 16,000 GA turbojets in service in the United States compared to about 8,750 today.⁷

While the numbers of GA turbojets is expected to increase dramatically over the next 10 years, it is important to bear in mind that small, single-engine aircraft will remain the large majority of the GA fleet by 2016. The FAA expects that over the next 10 years, propeller driven single-engine airplanes, two-seat light sport aircraft, and small home-built experimental airplanes will continue to make up more than 75% of the GA fleet.⁸ Security experts recognize that both the threats and vulnerabilities of these smaller aircraft are significantly different than the threats and vulnerabilities of medium and large sized GA turbojets and turboprops. Another segment of the GA industry is helicopters (rotorcraft), which make up only about 3% of the total GA fleet but are involved in several diverse and unique flight operations that introduce their own distinct set of security threats and vulnerabilities. The diversity of GA aircraft types and operations flown suggests that a one-size-fits-all approach to security is not practical – a tenet that both the GA industry and the TSA agree on.⁹

General Aviation Airports

Like GA flight operations and aircraft types, general aviation airports also vary significantly in their size and purpose and range from unpaved private airstrips with runways less than 2,000 feet in length located in remote, unpopulated areas to busy general aviation reliever airports situated in major metropolitan areas and converted military airbases with runways of sufficient length to handle the largest of jets.

In the United States, there are more than 19,000 total landing facilities including both public- and private-use facilities. Only about 450 of these airports serve regularly scheduled commercial passenger flights. The remainder consists of a wide variety of GA airports, heliports, and seaplane bases. Of these, almost 5,000 are public use, of which about 3,500 have paved runways. A large number of private use airports – over 4,500 out of about 14,000 total airports – also have paved runways. About 3,500 public use GA airports and another 1,000 private use landing facilities have lighted runways for night operations.¹⁰ The FAA's National Plan of Integrated Airport Systems (NPIAS) – a compilation of those airports eligible for federal Airport Improvement Program (AIP) funding because they are considered vital to the nation's aviation infrastructure – includes 278 GA reliever airports that primarily

⁷ Federal Aviation Administration. *FAA Aerospace Forecasts – Fiscal Years 2005-2016*. March 2005.

⁸ *Ibid.*

⁹ See Report of the Aviation Security Advisory Committee Working Group on General Aviation Airport Security (October 1, 2003); and Transportation Security Administration, *Security Guidelines for General Aviation Airports*. Information Publication A-001 (May 2004).

¹⁰ Federal Aviation Administration. *Administrator's Fact Book* (August 2005).

serve GA operations in major metropolitan areas, plus slightly more than 2,500 additional GA airports – mostly located in rural areas – that serve as critical links between various communities and the national airspace system. Only these airports are specifically eligible for federal AIP funds to implement security enhancements such as hangars to secure aircraft or improved perimeter fencing.

Airports that exclusively serve GA vary widely in terms of their proximity to densely populated areas, their levels of activity, and the types of operations conducted. To illustrate, consider Peachtree - Dekalb County Airport (PDK), a busy general aviation reliever located near Atlanta, Georgia. According to the FAA, PDK experiences an average of 639 operations per day, 64% by transient GA aircraft. According to a recent survey, PDK ranks 20th among the busiest GA airports in the United States.¹¹ While PDK has an air traffic control tower, even at this relatively busy airport, the tower closes during late night and early morning hours. Almost 600 aircraft are based on the field including 56 jets and 13 helicopters. Contrast this with Red Stewart Airfield (40I) in Waynesville, Ohio – a 2,400 foot long grass strip located roughly midway between Dayton and Cincinnati. The airport – considered an “uncontrolled field” because it has no operating control tower – sees less than 50 operations per day. The airport is home to only 44 aircraft – 40 small single-engine airplanes, 2 ultralights, and 2 gliders – that account for most (89%) of the flight activity at the airport.

Most security experts agree that applying identical or inflexible security measures at GA airports that vary so widely in their characteristics is likely to yield an unsatisfactory solution that could either overburden small airport operators or fail to mitigate potential vulnerabilities unique to specific airports or specific types of airports. Therefore, a risk-based strategy implementing security measures tailored to the unique characteristics and vulnerabilities of specific airports is generally thought to be preferable and has been advocated by aviation security experts and representatives from the GA industry.¹²

The Economic Impact of General Aviation

According to the FAA, general aviation directly generated \$13.7 billion and 178,000 jobs in 2000 and its overall economic impact was \$40.7 billion (roughly 0.4% of the Gross Domestic Product) and 511,000 jobs.¹³ The U.S. Government Accountability Office (GAO) provided a much higher estimate of the economic impact of GA, reflecting statistics often cited by the industry, stating that GA accounts for about 1.3 million jobs and contributes about \$100 billion to the U.S.

¹¹ General Aviation Manufacturers Association. *General Aviation Statistical Databook 2004* (Updated February 14, 2005). Washington, DC.

¹² See Report of the Aviation Security Advisory Committee Working Group on General Aviation Airport Security, and Transportation Security Administration, *Security Guidelines for General Aviation Airports*.

¹³ Federal Aviation Administration. *FAA Aerospace Forecasts, Fiscal Years 2005-2016*.

economy.¹⁴ While these larger figures probably take into consideration a broad reach of GA's indirect impact on travel and transportation-related business, the general picture provided by these various statistics is that GA is a relatively small but important component of the U.S. economy. As noted by the FAA, GA provides "on-the-spot efficient and direct aviation services to many medium and small-sized communities that commercial aviation cannot or will not provide."¹⁵ GA also plays an increasingly important role in training pilots and mechanics to serve the airline industry. Additionally, GA operations provide wide-ranging capabilities critical to our economy such as emergency medical services, overnight package delivery to small and mid-sized communities, helicopter transport to support oil drilling in offshore and remote locations, and the aerial application of pesticides to support agriculture.

The potential economic impact of security on GA could be quite significant. Since the terrorist attacks of September 11, 2001, GA airport operators and the industry have largely relied on their own initiatives and resources to implement security enhancements. These efforts have been somewhat limited because large scale security enhancements to protect GA assets across the country are expected to be rather substantial. For example, responding to criticism over a perceived lack of security at GA airports, Aircraft Owners and Pilots Association (AOPA) president, Phil Boyer, speculated "[w]e might be talking about \$40 billion to fence every small airport in this country, where in the world is that money coming from?"¹⁶ While a \$40 billion estimate may appear somewhat extreme – the TSA has spent slightly less than \$20 billion on all aviation security screening and enforcement at commercial airports in the four years since it was created following the 9/11 attacks – and erecting fences at every airport in the country may not be the most appropriate course of action, Boyer's concerns highlight the ongoing challenge of adequately funding GA security initiatives, balancing these initiatives with other homeland security needs, and doing so in a manner that does not create an undue economic burden on the GA industry. At the same time, the GA industry has a vested interest in implementing security measures to adequately secure and protect airplanes from theft and vandalism. A recent article in a GA trade publication noted that while the intent of tightening GA security has largely been seen as a means to prevent terrorism, "...a more immediate benefit could be a stronger bottom line for GA."¹⁷

The Aviation Security Advisory Committee (ASAC) Working Group on General Aviation Airport Security – an industry group assembled to assist the TSA in developing security guidelines for GA airports – concluded that "...a flexible, common-sense approach to general aviation airport security is mandatory if the

¹⁴ U.S. Government Accountability Office. *General Aviation Security: Increased Federal Oversight is Needed, but Continued Partnership with the Private Sector Is Critical to Long-Term Success*. (November, 2004) GAO-05-144.

¹⁵ Federal Aviation Administration. *FAA Aerospace Forecasts, Fiscal Years 2005-2016*. p. V-1.

¹⁶ Jim Hoffer. "Security Practically Non-Existent at Many Small Airports."

¹⁷ Robert Ross. "Keeping GA Safe and Secure." *Professional Pilot*, September 2005, p. 70.

industry is to retain its economic vitality and prosper.”¹⁸ Securing general aviation operations without incurring large costs and without imposing burdensome restrictions on legitimate general aviation operators is likely to remain a significant challenge for policymakers.

The Security Challenge

GA security poses significant challenges for policymakers and security experts because GA is highly diverse, geographically dispersed, and relatively open compared to commercial airports servicing passenger airlines and other protected infrastructure such as nuclear reactors and chemical plants. The security threat is not so much to GA assets themselves, but rather, from terrorists seeking to exploit GA assets to attack critical infrastructure or high profile targets. However, some GA assets could themselves become terrorist targets. For example, some corporate aviation operators have expressed concern that aircraft carrying high profile business leaders and executives, such as presidents of major U.S. corporations, could be targeted. Nonetheless, the primary threat identified regarding GA is the concern that aircraft may be used by terrorists to launch an attack against critical facilities or infrastructure.

A secondary threat is that terrorists may infiltrate or otherwise exploit GA to gain knowledge and/or access to the airspace system in the United States. It is known that some of the 9/11 hijackers trained in small GA airplanes in the United States before carrying out their attack using commercial jets. Consequently, following 9/11, there was a specific focus both from a law enforcement and a policy perspective on the security of flight schools within the United States. The Aviation and Transportation Security Act (ATSA; P.L. 107-71) originally called on the Department of Justice to implement a program to conduct background checks of all alien applicants seeking flight training in the United States in aircraft weighing more than 12,500 pounds and mandated security training for flight school employees. Vision 100 (P.L. 108-176) placed the responsibility for these flight school background checks in the hands of the TSA and expanded the program to include a notification requirement when foreign students initiate training in lighter aircraft weighing less than 12,500 pounds. These measures were enacted in direct response to the perceived threat that terrorists may infiltrate flight schools in order to gain operating knowledge of aircraft and the U.S. national airspace system.

Since September 11, 2001, policies toward broader GA security issues of protecting aircraft and airports from being exploited in terrorist attacks have focused on providing general guidelines and implementing cooperative arrangements between the GA industry and the TSA for carrying out security enhancements without imposing a rigorous statutory or regulatory framework. The GA industry has argued that inflexible statutory or regulatory measures could impose unnecessary burdens on certain sectors of the GA industry and could be extremely costly to carry out

¹⁸ Report of the Aviation Security Advisory Committee Working Group on General Aviation Airport Security. October 1, 2003. Department of Homeland Security, Transportation Security Administration, p. 3.

effectively. Legislative actions addressing GA security have focused primarily on the vetting of foreign flight school applicants, GA pilots, and more recently, prospective charter and lease customers. Regulatory actions have primarily focused on airspace restrictions and protections, mostly around the nation's capital, in addition to addressing statutory mandates for vetting certain individuals with access to GA airports and aircraft. Physical security of GA airports and aircraft has largely been left to aircraft owners and pilots, airport operators, and local authorities. While aircraft owners and pilots have generally favored this approach to avoid potentially restrictive federal security regulations, it has created a perceived burden on airport operators and local authorities to identify and address security needs at the airport level. The TSA has issued guidelines, largely based on industry recommendations, but the federal involvement in terms of both regulatory activity and funding for GA security initiatives has been relatively limited. This approach has led the media and some policymakers and security experts to voice concerns over what they perceive to be persisting vulnerabilities at some GA airports.

Security Vulnerabilities

Some media reports have raised significant concerns over what has been described as “practically nonexistent” security at many small general aviation (GA) airports.¹⁹ GA advocates have countered that small general aviation aircraft do not pose a significant threat and point out that many GA airports have taken reasonable steps, largely on their own initiative, to enhance security.²⁰ However, security concerns remain and a few high-profile incidents pointing to vulnerabilities in GA security have attracted considerable attention and raised concerns among some policymakers and security experts.

In the first of these high-profile incidents following the terrorist attacks of September 11, 2001, a student pilot intentionally crashed a small single engine airplane into a skyscraper in downtown Tampa, Florida on January 5, 2002. The pilot, described as a troubled youth, reportedly had expressed support for Osama bin Laden and the 9/11 terrorist attacks, but acted alone and had no known ties to any terrorist groups.²¹ More recently, on July 22, 2005, a small ultralight crashed near the German parliament building and Chancellor's office in Berlin in what was described by German air traffic control officials as a suspected suicide.²² The crash prompted German officials to establish a no-fly zone over central Berlin and again raised concerns in the United States over protecting key assets from possible attacks using

¹⁹ See, for example, Jim Hoffer. “Security Practically Nonexistent at Many Small Airports.” *WABC TV-New York Eyewitness News*, February 5, 2004.

²⁰ Aircraft Owners and Pilots Association. *General Aviation and Homeland Security: A Security Brief by the Aircraft Owners and Pilots Association*. Frederick, MD (January 23, 2004).

²¹ Vickie Chachere. “Police: Student pilot who crashed Cessna into Florida building inspired by bin Laden.” *Associated Press Newswires*, January 7, 2002.

²² David McHugh. “Small Plane Crashes Near German Parliament.” *Associated Press Newswires*, July 22, 2005.

GA aircraft as this incident occurred just over two months after a high-profile breach of the protected airspace around Washington, DC, by an unauthorized single-engine airplane that prompted evacuations of the White House and the U.S. Capitol.²³ While these incidents have received significant attention given the focus on aviation security following the attacks of September 11, 2001, GA aircraft have been used maliciously in earlier incidents of this kind. Most notably, in the early morning of September 12, 1994, a suicidal individual with a history of mental illness, reportedly despondent over personal and business problems, intentionally crashed a stolen small single-engine airplane on the south lawn of the White House.²⁴ While the small airplane was completely destroyed and the perpetrator was killed in the crash, property damage was minimal and the incident posed no threat to those in the White House.

Although these events have attracted substantial media interest, such incidents are relatively rare. While they identify real vulnerabilities in GA security, GA advocates caution that they should be properly viewed in the broader context of risk assessment which fully takes into account the security threat to critical infrastructure posed by these aircraft as well as the nature and scope of specific vulnerabilities. First, while each of these cases highlight the potential threat of general aviation aircraft, it is important to note that in each of these cases, damage caused by the aircraft was relatively limited and no injuries or deaths to persons on the ground occurred. Second, while the incidents in Tampa and Berlin and the 1994 White House incident point to a legitimate concern over suicidal pilots, a cursory review of National Transportation Safety Board (NTSB) aviation accident data revealed that since 1962, suspected suicides using GA aircraft are extremely rare, occurring at a rate of less than 2 incidents per year.²⁵ Perhaps more notably, none of these incidents resulted in any deaths of persons on the ground.

Recent high-profile thefts of GA aircraft in 2005 have also raised security concerns because they point to vulnerabilities in GA operations that could be exploited by terrorists. For example, in an incident that occurred on June 22, 2005, a 20-year old Connecticut man allegedly stole an aircraft from a Danbury, Connecticut flight school and took two teenage accomplices on a late-night “drunken, three-hour joyride” before landing on a taxiway at the Westchester County, New York airport.²⁶ More recently, on October 9, 2005, a 22-year old Georgia man allegedly stole a Cessna Citation VII business jet from the St. Augustine, Florida airport and took friends – reportedly unaware that the airplane had been stolen – on

²³ Hugh Williamson. “Ban on Small Aircraft Flying Over Berlin.” *Financial Times* (London), July 25, 2005.

²⁴ The White House Office of the Press Secretary. Press Briefing by Ron Noble, Under Secretary of the Treasury for Enforcement and Carl Meyer, Special Agent, United States Secret Service. September 12, 1994. Robert Pear. “Crash at the White House: The Pilot.” *The New York Times*, September 13, 1994, p. 20.

²⁵ CRS analysis of NTSB *Aviation Accident Database and Synopses* from 1962-2004 (available at [<http://www.nts.gov/ntsb/query.asp>]).

²⁶ Richard Liebson. “1 Held in Drunken Joy Ride in Cessna.” *The Journal News* (White Plains, NY), June 23, 2005, p. 1A.

a late-night joyride of more than 300 miles, landing at Gwinnett County (Georgia) - Briscoe Field airport near Atlanta.²⁷ While thefts of jets are extremely rare, in another incident that occurred on December 15, 1997, an individual with falsified FAA credentials stole a Lear Jet from the Fort Lauderdale Executive airport in Florida and piloted the airplane to Nicaragua to use the plane for charter flight operations.²⁸

Like suspected suicides using aircraft, thefts of small GA aircraft are relatively rare and thefts of jet aircraft are virtually unheard of. The AOPA notes that, historically, only about a dozen GA aircraft are stolen each year and recent trends suggest that owners and operators of these airplanes are taking steps to reduce their vulnerability to theft.²⁹ Specifically, the AOPA cites statistics from the Aviation Crime Prevention Institute, Inc. indicating that while 13 GA aircraft were stolen in 2002, only 6 (5 light single-engine aircraft and one medium-sized twin-engine aircraft) were stolen in 2003.³⁰ Arguably, these statistics do not indicate that GA aircraft are not vulnerable to theft, but rather may simply suggest that existing vulnerabilities in GA security are rarely exploited. While airplane thefts may be rare, high-profile thefts, like the cases cited above, provide some evidence that individuals with knowledge of GA airports and aircraft could exploit existing security vulnerabilities and access aircraft relatively easily.

The Terrorist Threat

While none of the events discussed above has been linked to terrorism, some limited intelligence information that has been made public suggests a continued terrorist interest in using GA aircraft to carry out attacks both domestically and overseas. For example, a crop duster pilot in Florida identified 9/11 suicide hijacker Mohammed Atta as an individual who had approached him in early 2001 inquiring about the purchase and operation of crop duster aircraft.³¹ Similarly, U.S. authorities presented evidence that Zacharias Moussaoui – who was arrested prior to the 9/11 attacks after raising suspicions surrounding his desire to train in large aircraft simulators and pleaded guilty to conspiring with the 9/11 hijackers – made similar inquiries about starting a crop dusting company while living in Norman, Oklahoma.

²⁷ Mike Morris. “Bufurd Man, 22, Accused of Stealing Jet.” *The Atlanta Journal-Constitution*, October, 12, 2005.

²⁸ U.S. Department of Justice. Marcos Daniel Jiménez, United States District Attorney for the Southern District of Florida. “Defendant Sentenced for Transporting Stolen Lear Jet and Possession of False Identification Documents.” Press Release, January 5, 2005: Miami, FL.

²⁹ Aircraft Owners and Pilots Association. *General Aviation and Homeland Security*.

³⁰ *Ibid.*; Testimony of Mr. Andrew Cebula, Senior Vice President, Government and Technical Affairs, Aircraft Owners and Pilots Association, Before the Senate Committee on Commerce, Science, and Transportation Regarding General Aviation Security, June 9, 2005.

³¹ Statement for the Record of Robert S. Mueller III, Director, Federal Bureau of Investigation, Before the Joint Intelligence Committee Investigation into September 11, U.S. Congress, June 18, 2002

Evidence was also presented that Moussaoui was in possession of a computer disk containing information regarding the aerial application of pesticides.³² This evidence raised concerns at the Central Intelligence Agency (CIA) that al Qaeda has “considered using aircraft to disseminate [biological warfare] agents.”³³

The CIA also suggested that, in initially planning the 9/11 attacks, one of Osama bin Laden's associates proposed that the World Trade Center be targeted by small aircraft packed with explosives, but bin Laden himself altered the plan to use large commercial jets instead.³⁴ If true, this suggests that terrorists engaged in some deliberative process of weighing the pros and cons of general aviation as compared to commercial airlines in planning the 9/11 attacks. While the terrorists favored commercial aircraft in carrying out their attack on September 11, 2001, in the post-9/11 environment, heightened security measures at commercial airports could make GA assets considerably more attractive to terrorists than in the past. While it is unlikely that small GA aircraft packed with conventional explosives could cause the amount of destruction inflicted on September 11, 2001, large jet aircraft in the GA fleet or smaller aircraft carrying chemical, biological, radiological, or nuclear (CBRN) weapons may pose a more formidable threat.

Although no publically available intelligence on terrorist operations since September 11, 2001, has indicated any specific threat involving GA aircraft domestically, evidence indicates that al Qaeda has maintained a continued interest in using small aircraft to attack U.S. interests overseas. For example, on April 29, 2003, Pakistani authorities apprehended Waleed bin Attash (a.k.a., Khallad, Tawfiq bin Attash), the suspected mastermind of the U.S.S. Cole bombing and a known associate of the 9/11 hijackers, and five other suspected al Qaeda operatives in Karachi, Pakistan. Soon after the arrests, authorities uncovered a plot to crash a small, explosives-laden airplane into the United States consulate office in Karachi illustrating al Qaeda's continued interest in using aircraft to attack U.S. assets.³⁵ The DHS subsequently issued a security advisory indicating that al Qaeda was planning to use GA aircraft to attack warships in the Persian Gulf as well as the U.S. Consulate in Karachi, Pakistan. While the advisory characterized these threats as a demonstrated “fixation” on using aircraft in attacks against U.S. assets, it was strongly criticized by GA interests as being overly alarmist and overstating the potential threat posed by small GA aircraft.³⁶

³² United States of America v. Zacharias Moussaoui (Defendant). Indictment. In the U.S. District Court for the Eastern District of Virginia, Alexandria Division. December 2001 Term.

³³ U.S. Central Intelligence Agency. *Terrorist CBRN: Materials and Effects*.

³⁴ U.S. Central Intelligence Agency. Unclassified Version of Director of Central Intelligence George J. Tenet's Testimony before the Joint Inquiry into Terrorist Attacks Against the United States, 18 June 2002.

³⁵ Associated Press. “U.S. Uncovers Al-Qaida Plot in Pakistan; The Terrorist Group Allegedly Planned to Fly an Airplane into the American Consulate.” *Telgraph-Herald* (Dubuque, Iowa), May 3, 2003, p. A7.

³⁶ *Ibid.*

Risk Factors Associated with General Aviation

In examining the security risk posed by aircraft that could be utilized in suicide attacks or as launch platforms for conventional weapons, the threat posed by general aviation aircraft is largely a function of aircraft weight, payload capacity (including fuel capacity), and speed. Other factors would likely play a relatively small role in the overall threat posed by particular aircraft. For example, aircraft agility – a rough measure of its capability to maneuver and evade countermeasures – may be considered a factor in the risk equation, albeit a relatively minor one. A small two-seat sport aircraft might be quite agile, but its small size, relatively slow speed, and limited payload capacity may significantly limit the threat posed by such an aircraft. GA interests point out that most GA aircraft are capable of carrying less payload than a typical light car.³⁷ For example, both the Cessna 172 and Piper Warrior – very popular single-engine aircraft – have maximum takeoff weights of less than 2,500 pounds and useful payloads (including allowances for fuel and passengers) of less than 1,000 pounds.³⁸ By contrast, the truck bomb used in the April 19, 1995, Oklahoma City bombing was believed to have contained about 5,000 pounds of improvised explosives and the truck bomb involved in the February 26, 1993 bombing at the World Trade Center in New York City was believed to contain a 1,300 pound device. While these events involved unusually large explosive devices, typical light GA aircraft would only be able to carry a device a small fraction of this size. Thus, at least with regard to being used as a platform for conventional explosives, the threat posed by light GA aircraft is relatively small compared to trucks which have significantly larger payload capacities.³⁹

However, as ground based security measures such as setbacks, barriers, and access controls are implemented around critical infrastructure, terrorists may view GA aircraft as a possible means to circumvent these defenses. While many forms of ground transportation, especially trucks, can accommodate significantly larger payloads than almost all GA aircraft, some observers fear that aircraft may be used in a terrorist attack because they cannot be as easily thwarted by blockades, barriers, or other physical security measures. Nonetheless, executing an attack that involves loading a GA aircraft with a large quantity of explosives may be difficult without raising some suspicion at the airport, at least domestically where airport operators and pilots have been instructed to be vigilant for such unusual activities.

While the threat posed by light GA aircraft carrying conventional explosives is limited by the size and speed of these aircraft, some experts argue that small aircraft

³⁷ Aircraft Owners and Pilots Association. *General Aviation and Homeland Security: A Security Brief by the Aircraft Owners and Pilots Association*. (January 23, 2004, Frederick, MD).

³⁸ Based on information from Cessna Aircraft Company, *Information Manual: Skyhawk Model 172P*, May 12, 1981, and Piper Aircraft Corporation, *Piper Warrior II Information Manual*, Revised September 12, 1990.

³⁹ While weight is not the only consideration in evaluating explosive force, it is meaningful for comparing the potential threat posed by aircraft and vehicles that differ in terms of their payload capacity.

may pose a significant threat if used as a platform to launch a chemical, biological, radiological, or nuclear (CBRN) attack over a densely populated area. In these cases, payload capacity and speed may not be considered as significant components of the risk equation. Rather, with regard to the CBRN threat, the most significant element associated with small GA aircraft appears to be their unique capability to fly at relatively low altitudes above densely populated areas and large congregations of people on the ground. In fact, the slow speed of these smaller aircraft and the ease at which doors and windows on non-pressurized airplanes and helicopters can be operated in flight may actually pose a greater threat of certain types of attacks, such as chemical and biological attacks, as compared to larger, faster aircraft. Agricultural aircraft used for spraying crops with pesticides and fertilizers pose a unique threat as a platform for a biological or chemical attack because they are specifically designed for aerial dispersal and could be exploited by terrorists for this specific purpose.

However, the chemical and biological threat using GA aircraft may not be as ominous as some fear. First, many chemical agents must be released in rather high concentrations. Some, such as cyanides, may only be effective as a chemical weapon if dispensed in an enclosed area therefore greatly limiting the threat of aerial dispersion.⁴⁰ While other chemical agents – such as caustic mustard agents and military nerve agents – may be effective in open air settings, the limited payload of small GA aircraft may limit the scope of an aerial attack using such agents. Second, aerial dispersion of either chemical or biological agents over populated areas or large congregations of individuals is likely to be easily detected. If a suspected aerial dispersion of a chemical or biological agent is promptly reported, a timely public health response could significantly limit the impact of such an attack. In general, experts believe that if any chemical or biological attack were to occur – whether using a small airplane or some other method to attack – it would likely be on a small scale physically, but may have a large psychological impact on the population.⁴¹

More specifically, in terms of using small GA aircraft to carry out such an attack, the greatest threat appears to be to large, open-air assemblies such as major outdoor sporting events and concerts. In fact, one of several homeland security planning scenarios – developed by the White House Homeland Security Council in partnership with the DHS – describes the potential effects of an adversary using a light aircraft to spray a chemical blister agent into a packed college football stadium holding 100,000 people.⁴² The scenario's predicted impact includes 70,000 hospitalizations due to exposure, including many permanent impairments and 150 deaths, but notes that expedient decontamination could reduce injuries by one half. This would likely be a worst case scenario in which an extremely large assembly of people could potentially be victimized. Even in densely populated areas, this degree of impact from an aerial attack not specifically targeting a large outdoor assembly is unlikely because it might be expected that many individuals would be indoors or

⁴⁰ U.S. Central Intelligence Agency. *Terrorist CBRN*.

⁴¹ See CRS Report RL31831, *Terrorist Motivations for Chemical and Biological Weapons Use: Placing the Threat in Context*, by Audrey Kurth Cronin.

⁴² White House Homeland Security Council, David Howe, Senior Director for Response and Planning. *Planning Scenarios: Executive Summaries* (July 2004, Version 2.0).

adequately protected by buildings and other structures. Nonetheless, while such an attack may be limited in terms of its physical impact, it may cause widespread fear and panic.

By comparison, the threat from radiological and nuclear devices appears to be much greater in terms of the potential for mass casualties and physical destruction. A small-scale explosive radiological dispersal device – a so-called “dirty-bomb” – could easily fit inside a backpack,⁴³ and a pilot carrying such a device on to a small airplane may not arouse any particular suspicion at an airport. However, the threat from such devices is not unique to GA aircraft as these devices could reach their intended target by other means, including being carried in a small car or even being carried by a pedestrian. Most experts concede that, once in the hands of terrorists, it may be difficult to stop an attack with a radiological or nuclear device because many options are available to deliver the weapon to its intended target. Using GA aircraft is one of many means for launching such an attack. However, there is no reason to believe that GA aircraft are any more appealing to terrorists nor any more vulnerable than other possible methods of attack.

Concerns have also been raised over the potential threat that an aircraft attack may pose to a nuclear power plant, a chemical plant, or other potentially vulnerable infrastructure where a terrorist attack could inflict widespread damage and mass casualties. A review of security measures at nuclear reactors prepared by the office of Representative Markey identified several perceived vulnerabilities at nuclear reactor sites suggesting that these facilities may be vulnerable to 9/11-style attacks using general aviation aircraft. Based on information provided by the Nuclear Regulatory Commission, Representative Markey’s office issued a report on nuclear reactor security that included an assessment of the vulnerability of these facilities to an attack by aircraft.⁴⁴ The report noted that while 21 out of 103 reactors in the United States are located within 5 miles of an airport, 96% of U.S. nuclear reactors did not factor the impact from even a small aircraft into their design. Four reactors were evaluated during their design to consider impacts from aircraft weighing up to 12,500 pounds which would include most GA aircraft except for business jets and large twin engine aircraft. Three Mile Island in Pennsylvania was cited as the only facility where portions were designed to withstand the impact of large airliners in addition to smaller aircraft. In contrast, the report noted that some European countries, including Switzerland and Germany in particular, incorporate safety features such as reinforced concrete walls and spatial separation of critical safety systems to withstand the crash of certain types of military and commercial aircraft.

Other examinations of the potential threat to nuclear facilities from aircraft have focused on perceived vulnerabilities of spent-fuel pools used to cool expended nuclear fuel. However, power companies maintain that a study modeling the impact

⁴³ U.S. Central Intelligence Agency. *Terrorist CBRN*.

⁴⁴ Staff Summary of Responses by the Nuclear Regulatory Commission to Correspondence from Rep. Edward J. Markey (D-MA), Member, Energy and Commerce Committee, U.S. House of Representatives. *Security Gap: A Hard Look At the Soft Spots in Our Civilian Nuclear Reactor Security*. March 25, 2002.

of an aircraft crash into a spent-fuel pool wall concluded that while such a scenario could crush or crack the wall, it would not likely cause a release of radiation⁴⁵.

A report prepared for the AOPA by Robert Jefferson, a nuclear reactor safety consultant, concluded that the threat to nuclear reactors from small general aviation aircraft is “practically non-existent” and “...it is unlikely that a terrorist would choose a light general aviation vehicle to threaten a nuclear power plant.”⁴⁶ Jefferson’s analysis concluded that even the impact of an airliner like those used in the 9/11 attacks would, in all likelihood, be unable to penetrate the outer containment vessel and argued that the analysis referenced by Representative Markey significantly overstates the risk potential and “...overlooks the fact that by their very design, nuclear power plants are inherently resistant to [airborne attacks].”⁴⁷ The report also concluded that the proximity of nuclear reactors to GA airports does not increase the exposure of these facilities to terrorist threats.

Although the specific threat posed to nuclear facilities by GA aircraft remains a contentious issue, the FAA has kept in force restrictions on circling, loitering, or otherwise flying in a suspicious manner around nuclear facilities. Arguably, these measures would provide little deterrent against a well-planned terrorist attack. However, they highlight the continued concern over possible airborne threats to nuclear facilities, whatever the true risk may be. More elaborate measures to protect nuclear facilities, such as implementing anti-aircraft defense capabilities around nuclear facilities, are wrought with operational and policy complexities including high costs, questionable effectiveness, and a potentially high risk of shooting down an errant GA pilot who meant no harm.

While light GA aircraft appear to pose a relatively limited threat by themselves in terms of physically damaging critical infrastructure, larger GA aircraft pose a potentially more formidable threat. Due to the size and speed of some of these aircraft, particularly mid-sized and large business jets, they could inflict significant damage on buildings and critical infrastructure if used in a suicide attack. These aircraft have significantly larger payload and fuel capacities which would have a direct bearing on the degree of physical damage they could cause to buildings and infrastructure. Thus, in terms of both assessing risk and identifying options for mitigating the security risk posed by GA, the distinction between small GA aircraft that make up the large majority of the fleet and larger business jets has important implications. While small aircraft appear to pose a greater threat as possible platforms for chemical or biological attacks, large business jets appear to pose more of a threat from being exploited in a suicide attack scenario similar to the September 11, 2001, attacks using commercial airliners. Because the various sectors of GA appear to pose distinct threats, risk mitigation strategies arguably should be tailored to some degree to address the specific security threats posed by different sectors of

⁴⁵ Gary Stoller. “Nuclear Plants near Airports May Be at Risk.” *USA Today*, June 10, 2003.

⁴⁶ Robert M. Jefferson. *Nuclear Safety: General Aviation Is Not a Threat* (May 16, 2002), p. 4 and p. 1. Available from Aircraft Owners and Pilots Association, Frederick, MD.

⁴⁷ *Ibid*, p. 1.

the GA industry as well as the specific nature of potential security vulnerabilities that also vary across different types of aircraft and flight operations.

Possible Options to Mitigate the Security Risks of General Aviation

A variety of options exist for mitigating security risks posed by GA aircraft and flight operations, many of which have been implemented or are currently under development or consideration. As previously discussed, the selection of mitigation options may need to be tailored to specific vulnerabilities and threats of different sectors of the GA industry which may differ significantly in their degree and scope. While a wide range of options are available, many of the more extensive and costly options for providing security may not be economically feasible, practical, or necessary at smaller GA airports away from major population centers. Several available options center on traditional security techniques to improve access controls and surveillance around GA facilities and better protect aircraft against theft and unauthorized use. Additional options include procedures for vetting individuals with authorized access to aircraft and aviation facilities, and procedures for clearing passengers. Another possible option for enhancing GA security would be to address law enforcement and homeland security response to suspicious activities and improved intelligence tracking of such incidents to identify patterns indicative of possible terrorist activity. Finally, in terms of adopting a layered security system to augment measures put in place at airports, airspace restrictions and defenses may be considered to protect high-profile sites and critical infrastructure from the threat of aerial attacks.

Costs, in terms of direct implementation and oversight costs as well as the indirect costs related to disruption of air commerce and freedom of movement, are likely to be important considerations in assessing the utility and feasibility of implementing specific options to enhance GA security. For example, implementing broadly applied security requirements for all GA airports may impose significant cost challenges, particularly to small, rural airports where the need for such measures may be questionable. Also, airspace restrictions tend to be highly contentious because while they directly impact air commerce and the freedom of movement, they are viewed by some experts as being of questionable value in preventing a terrorist attack unless coupled with elaborate air defense capabilities. Deploying air defense capabilities on a large scale to protect against possible aircraft attacks carries a relatively high cost and involves extensive commitments of resources and collaboration between the FAA, the DHS and the Department of Defense (DoD). The costs and benefits associated with various mitigation options can be analyzed in a risk analysis framework – examining the threat and vulnerability of specific sectors of the GA industry – to better understand the tradeoffs between various options.

Because of the diversity of GA airports, aircraft, and flight operations, and the varied threats and vulnerabilities posed by different sectors of the GA industry, a logical starting point in mitigating security risk would be to perform systematic risk analyses or security risk assessments examining specific components of GA. The FY2006 Department of Homeland Security Appropriations Act (P.L. 109-90)

contains a provision requiring the DHS to examine the vulnerability of high-risk areas and facilities to possible attack from GA aircraft. This mandate focuses on the specific vulnerability of critical infrastructure to attack, which relates more closely to the threat to critical infrastructure and other significant sites posed by GA aircraft as discussed in this report. In this report vulnerability has referred instead to the specific weaknesses in security measures to protect GA airports and aircraft that could be exploited to gain unauthorized access to facilities and aircraft. A comprehensive risk assessment and risk mitigation strategy would likely take into account both the threat and vulnerability associated with GA operations as well as the potential cost of consequences associated with possible terrorist attack scenarios.

Security Risk Assessments

Security risk can be viewed as a function of: 1) the threat or threats posed by a specific type of flight operation or activity measured in terms that attempt to quantify the probability of various terrorist attack scenarios; 2) the vulnerability or susceptibility of existing security weaknesses measured in probabilistic terms reflecting the likelihood that they could be exploited by terrorists; and 3) the possible consequences measured in terms of predicted damage or associated cost. Using this risk analysis framework, the relative effectiveness of mitigation options can be evaluated in terms of how specific security enhancements might reduce vulnerability and how resources could be allocated in a manner to mitigate threats based on their likelihood and their potential consequences. The anticipated risk reduction can then be compared to expected costs in an attempt to determine the most cost effective strategies for enhancing GA security.

For passenger airline operations, a layered approach to aviation security has been implemented. This layered system includes passenger name checks against watch lists, passenger and baggage screening, access controls at airports, hardened cockpit doors, and armed air marshals and pilots on passenger airlines. The layered approach has a unique advantage in reducing vulnerability by adding additional safeguards to foil terrorists, thereby greatly reducing the overall vulnerability of the entire system. In probabilistic terms, the vulnerability of the entire security system is the combined or joint probability that each individual layer could be breached or circumvented. Thus, while the threat of terrorism still exists, most experts would agree that, in the case of passenger airlines, the risk of terrorism has been significantly mitigated by greatly reducing the vulnerability that security weaknesses could be exploited by terrorists through the implementation of a multi-layered security system.

In the case of GA, a systematic examination of security risk has not been completed. However, many experts acknowledge that various security vulnerabilities and threats exist. An analysis of GA security by the International Civil Aviation Organization (ICAO) concluded, “[t]he challenge of designing general aviation security measures focuses on the need to thoroughly define the threat. Before

security standards can be developed, there must be a clear picture of the problem.”⁴⁸

One challenge often cited and already noted in this report is the diversity of GA airports. In many respects, the characteristics of GA airports are much more diverse than those of commercial passenger airports. Yet recognition of this diversity is not always acknowledged in discussions of GA security risk. In contrast, commercial passenger airports are stratified in a tiered system based on their security needs: commercial airports are placed into one of five categories (Category X, I, II, III, IV) based on factors such as the volume of passengers, the level of international operations, and the proximity to critical locations like Washington, DC. A similar model could be adopted to categorize GA airports based on their security risks and the particular security needs of certain classes of GA airports, or in some cases for specific operators of large fleets of GA aircraft. Toward this goal, the TSA provided as part of its security guidelines for GA airports an airport characteristics measurement tool where airports are scored based on a variety of factors including their proximity to metropolitan areas and sensitive sites; surrounding airspace; the number of based aircraft; runway lengths; the numbers and types of flight operations; and the presence of maintenance, repair, and overhaul (MRO) facilities.⁴⁹ Using this tool, airports are scored on a scale ranging from 0 to 64. Based on the scoring, airports will fall within one of four bands, and the TSA has provided suggested security enhancements for each of the four bands. However, because use of this assessment tool is voluntary, and because the process is relatively generic and does not consider site-specific factors, it provides only a rudimentary risk assessment tool and process for GA airport operators.

While the requirement established under the FY2006 Department of Homeland Security Appropriations Act (P.L. 109-90) mandates a broad examination of the security threat posed by GA, more detailed security risk assessments can be done either at the airport level or, for some larger operators, such as fractional-ownership fleets, at the operator level. Due to the diversity of GA airports and the kinds of operations that they accommodate, the risk picture is likely to vary widely. For example, some small airports in mid-western and mountain states might have few security measures in place and therefore may be considered vulnerable. However because of their remote location – away from major population centers – these airports may pose little threat. On closer examination, it may be found that such airports may not be particularly vulnerable to terrorist infiltration based on several factors. For example, a remote location away from any high-profile sites or densely populated areas might not be particularly attractive to terrorists, and the close-knit community of airport users in small, rural communities may be more likely to spot outsiders and detect suspicious activity. On the other hand, a busy GA reliever airport near a major metropolitan airport may pose a greater risk. Even if such an airport has implemented various security measures to mitigate risk, it may still be regarded as more vulnerable than a rural airport because terrorists may be able to more easily blend in with large numbers of individuals accessing the airfield, and

⁴⁸ Donald Spurstun. “Security Requirement for GA Operations Should be Based on Threat Assessment.” *ICAO Journal*, Number 8, 2002, p. 18.

⁴⁹ Transportation Security Administration. *Security Guidelines for General Aviation Airports*. Information Publication A-001, May 2004.

while some access controls may be in place, they may not be adequate for preventing motivated terrorists from circumventing these measures or exploiting weaknesses in access controls.

The TSA's approach to risk assessment to meet the sector-specific security plans called for in *Homeland Security Presidential Directive(HSPD)-7: Critical Infrastructure Identification, Prioritization, and Protection* is the ongoing development of a Vulnerability Information Self Assessment Test (VISAT) for GA airports. VISAT programs have already been developed for other transportation infrastructure including maritime, rail, bridges, and mass transit, and others are under development for other transportation sectors including rail and trucking HAZMAT.⁵⁰ The GA VISAT, currently under development, is designed to be a self-guided, computer-based assessment tool designed to assess risk and mitigation at GA airports. However, this TSA approach to assessing security risk at GA airports has been criticized over its lack of understanding and differentiation of GA from the air carrier environment and its extensive reliance on standards developed for nuclear power plant security that do not adequately address the public access needs of GA airports.⁵¹ Critics have argued that the TSA should instead, incorporate more updated threat and risk management standards developed by FEMA that more fully address public access needs.⁵² While some of these recommendations may be incorporated into the final assessment tool issued by the TSA to assess security risk at GA airports, a comprehensive, standardized tool to perform detailed analyses of security risks in the GA sector does not currently exist. Many experts believe that such a tool could be extremely beneficial for identifying risks and designing security programs for specific airports or specific categories of GA airports.

Based on detailed analyses, cost-effective security programs that address the specific degree and nature of risk at specific airports can be designed and implemented. Various combinations of security measures are available and can be tailored for airport-specific or operator-specific security plans. These include various approaches to: surveillance and monitoring; airport access controls; and physical security measures to protect aircraft. These specific security systems implemented by airports and operators may be augmented by broader initiatives such as the vetting of GA pilots and airport workers at the federal level and establishing specific procedures and defenses to protect airspace near critical locations such as key federal facilities in Washington, DC. In the following discussion, these various approaches and the challenges associated with applying them to GA security are analyzed in further detail.

⁵⁰ Transportation Security Administration. *DHS-Vulnerability Identification Self-Assessment Tool (VISAT)*.

⁵¹ Robert Olislagers. "General Aviation Security: The Ups & Downs of Threat Management." *Airport Magazine*, May/June 2005, pp. 59-61.

⁵² *Ibid.*

Surveillance and Monitoring

Surveillance and monitoring of GA operations is a challenge. Of the 5,286 public use landing facilities in the United States, only about 500 have operating control towers and most of these are located at airports with regularly scheduled commercial service. Only the busiest airports that cater exclusively to GA aircraft have operating control towers. These airports usually are geographically large and congested making surveillance for security purposes from the tower difficult. What's more, even at the limited number of GA airports with operating control towers, most towers are not operated on a continuous basis and close during late night and early morning hours. While language in a Senate-passed amendment to the FY2006 DHS Appropriations bill (see S.Amdt. 1106 to H.R. 2360) would have required "an assessment of whether unmanned air traffic control towers provide a security or alert weakness to the security of general aviation aircraft", the security role of staffed control towers is unclear. During operating hours, controllers remain busy performing air traffic separation and control functions, making it difficult for them to spot unusual activity or detect unauthorized aircraft usage unless suspicions are raised by unusual requests, improper phraseology, or procedural violations. Therefore, the mere presence of a operating control tower appears to provide little additional security to a GA airfield.

Smaller GA airports, most of which do not have operating control towers, are usually not attended by airport management or fixed-base operators (FBOs) on the field 24 hours a day. Depending on the frequency of traffic, an airport may be attended only during daylight hours, or sometimes during limited evening hours. Aircraft may still use many of these airports during late night and early morning hours as runway lights can be controlled from the cockpit using onboard radios. Airport access controls and surveillance during these unattended hours presents a unique challenge to airport operators. On the one hand, accessibility is important to meet the needs of air commerce by allowing operations such as late night arrivals and departures for business trips and overnight cargo delivery to small communities. Furthermore, maintaining airport accessibility at night provides a critical safety function allowing pilots sufficient alternate landing sites if required to deviate for weather or mechanical reasons. Providing adequate site security for GA airports while allowing airport access for these purposes, including access for transient aircraft, presents a daunting challenge.

Full time security is a costly option for many small airports. Remote sensing and surveillance using cameras and motion sensors, for example, may offer a somewhat more cost effective alternative, but requires close coordination with local security forces and law enforcement to respond to suspected threats or security breaches. Uncertainty and high false alarm rates in detection systems can drive up costs associated with security response and can lead to complacency that may limit the effectiveness of these systems. However, these remotely monitored security systems provide an alternative to security monitoring for many airport sites where full time on-site security is cost prohibitive. At least one vendor provides tailored security packages, integrating alarms, cameras, entry and access controls, fencing,

lighting, and motion and acoustic sensors.⁵³ A key element of these types of integrated security systems are their monitoring capabilities, including remote internet-based monitoring of cameras and other intrusion detection devices, and the capability to tie into local law enforcement networks for coordinated response. However, these integrated systems can be quite costly to install, maintain, and operate. Consequently, the GA community, in coordination with the TSA, has applied a long-established method of providing security and surveillance in residential neighborhoods – the neighborhood watch concept – to GA airports throughout the United States.

Airport Watch Program. To enhance surveillance at airports, the TSA, in cooperation with the AOPA and the National Response Center, launched an airport watch program at GA airports in December, 2002.⁵⁴ The airport watch program is similar to a neighborhood watch program and relies on the cooperation and participation of pilots, airport tenants, and airport workers to observe and report suspicious activity. Educational and training materials have been made available to these individuals to increase their awareness regarding potentially suspicious activity, and a hotline – 1-866-GA-SECURE – has been set up to log reports of suspicious activity. Under the program, instructional materials advise observers to call local law enforcement using 911 if they believe the situation potentially poses an immediate threat. The AOPA has provided funding and resources since the program's inception to provide educational and informational materials for pilots and for signage – similar to neighborhood watch signs – at airports. According to the AOPA, the organization has spent more than \$1 million from its own funds developing, promoting, and providing support for the Airport Watch Program.⁵⁵ Congress has supported the Airport Watch program in appropriations language, and the FY2006 Department of Homeland Security Act (P.L. 109-90; H.Rept. 109-241 and H.Rept. 109-79) provides an additional \$275,000 for additional promotion of the program.

Since its inception, the Airport Watch program has been credited with alerting authorities to suspicious activities at GA airports on several occasions. For example, the AOPA cited one peculiar incident as a demonstration of the effectiveness of the airport watch concept. In August 2004, two men of “Middle Eastern appearance” presented themselves at an airport near St. Louis offering cash to charter a helicopter and presenting driver's licenses from two different states as identification. The charter operator also noted that the men were driving a vehicle registered in a third state and observed the men removing “odd shaped luggage” from that vehicle in preparation for the flight. Based on these observations, the charter operator stalled the suspicious individuals and notified the FBI and local law enforcement who responded and arrested the two individuals. The suspicious characters turned out to be reporters on assignment to demonstrate how easily terrorists could hijack a

⁵³ Robert Ross. “Keeping GA Safe.”

⁵⁴ Transportation Security Administration. “General Aviation – Hotline.”

⁵⁵ Testimony of Mr. Andrew Cebula, Senior Vice President, Aircraft Owners and Pilots Association. Before the Senate Committee on Commerce, Science, and Transportation on General Aviation Security, June 9, 2005.

helicopter.⁵⁶ The AOPA noted several other successes of the Airport Watch program including the capture of a suspected con man in Kansas who attempted to rent aircraft at several facilities, and several cases of suspicious inquiries regarding aircraft rentals, charter flights, flight instruction, and use of hangar storage space. These incidents all resulted in responses by federal law enforcement authorities, although none have been specifically linked to terrorism.⁵⁷

Despite the benefits and successes of the Airport Watch Program, which have been achieved at a relatively low cost, there are several challenges to implementing a successful watch program. A major limitation of the Airport Watch Program is that it may be difficult – especially for untrained observers – to distinguish suspicious behavior from normal activities. Past terrorist attacks have indicated that terrorists are likely to use methods that avoid arousing suspicion. In essence, terrorists have in the past hid in plain site and may be likely to do so in the future.

In the case of general aviation, the all too obvious example of a clandestine rendezvous where cargo is loaded from a suspicious vehicle on to a small aircraft at a remote area of the airport may likely be regarded as too risky by terrorist groups to attempt. Rather, terrorists may try to blend in as well as possible. This could lead to two undesired consequences: high false alarm rates and racial and ethnic profiling by well intentioned pilots and airport tenants. High false alarm rates could place a strain on local law enforcement, especially in rural areas and small communities where law enforcement support is limited. Other limitations to these types of programs are that the response time of local law enforcement is often slow, and local law enforcement – especially in small, rural communities – may not be adequately integrated with homeland security systems to receive a timely notification when an incident is reported, although observers are specifically instructed to dial 911 if they believe the situation poses an immediate threat. Another difficulty is that local law enforcement may become complacent if a large number of false alarms are reported at local airports. Despite these obvious limitations, Airport Watch is regarded by many as a model program in the sense that it raises awareness and provides a relatively inexpensive means of providing surveillance. The program could potentially be improved by providing more detailed information and training to pilots, airport tenants, and airport workers in observational techniques – such as behavioral pattern recognition – to improve the quality of information provided to the Airport Watch hotline or relayed through other notification channels.

Behavior Pattern Recognition. One challenge in implementing an Airport Watch Program is that it is highly dependent on the observations and reporting of untrained individuals. This difficulty is compounded by the fact that suspicious terrorist activities may not appear out of the ordinary to the casual observer. While convicted terrorist Zacharias Moussawi's peculiar inquiries about flying large jet aircraft and his obvious lack of qualifications to seek such training did raise suspicions at the flight school where he sought advanced jet training, terrorist behavior patterns are likely to be much more subtle. None of the 9/11 terrorist pilots

⁵⁶ Aircraft Owners and Pilots Association. *Proof AOPA Airport Watch Concept Works*. August 12, 2004. Frederick, MD: AOPA.

⁵⁷ See Testimony of Mr. Andrew Cebula.

nor Mossaoui attracted similar attention during their initial training in small GA aircraft. Qualified pilots seeking to rent light aircraft also may attract little attention and a pilot loading a small single-engine airplane with dangerous chemicals or biological agents may look no different than a pilot loading his personal effects on board for a weekend getaway. While single incidents like this typically arouse little suspicion, aggregate behavior that might appear somewhat odd or suspicious could collectively signal possible terrorist or criminal activity.

An additional downside of programs like the Airport Watch Program is that they could result in unintended racial or ethnic profiling by well intentioned observers. For example, would the individuals in the St. Louis incident cited by AOPA have raised similar suspicions if they were not of “Middle Eastern appearance”? Besides the potential for falsely targeting individuals in certain racial and ethnic groups, there is also the danger that, conversely, untrained observers may not notice suspicious behavior patterns exhibited by other individuals. Intelligence sources suspect that al Qaeda is seeking to recruit non-Middle Eastern individuals for the very reason that they may be less likely to raise suspicions. More specific guidance and training to airport workers, tenants, and pilots could improve the effectiveness of the Airport Watch Program and other surveillance operations.

A possible solution to overcome some of these limitations involves the implementation of behavioral pattern recognition techniques. As described in a recent commentary on GA security, behavioral pattern recognition was highlighted as being “...designed to maximize detection while minimizing, if not eliminating, issues of civil liberties.”⁵⁸ Behavioral pattern recognition – which is in use at airports worldwide and has been highlighted in numerous profiles of Israel’s El Al airlines’ pre-boarding security screening – examines deviations from normative behavioral patterns. It has been suggested that behavioral pattern recognition could be applied in the GA environment by providing specific training to maintenance and line workers, for example, making them an integral part of an airport’s security network rather than having a small number of employees responsible for security.⁵⁹

One challenge in behavioral pattern recognition is that single events may not stand out, but aggregate samples of slightly unusual activity may provide tell-tale signs of preparations for launching a terrorist attack. However, assimilating and correctly interpreting this data remains a significant challenge. For this reason, a “reporting tree”⁶⁰ is recommended for guiding decisions about responding to suspicious behavioral patterns. The “reporting tree” concept is integrated into the TSA’s security training for flight schools, which is a required security training element for flight school employees under Title 49, Code of Federal Regulations, §1552.21 *et seq.*, but has not yet been expanded to other aspects of GA security. A reporting tree might include notifying a supervisor, such as a chief flight instructor or flight school manager, about strange inquiries or behaviors by a student pilot, and escalating this information up the reporting tree to law enforcement or federal

⁵⁸ Robert Olislagers. “General Aviation Security.”, p. 61.

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

officials only if the behavior is repeatedly demonstrated and, in aggregate, raises enough concern that it warrants further action. In this manner, the Airport Watch program, in coordination with specific training and guidance in techniques such as behavioral pattern recognition and the use of reporting trees, has the potential to contribute to the intelligence gathering function at a relatively low cost by enlisting the support of a broad segment of the GA community.

Airport Access Controls

Controlling access to general aviation airports is a significant challenge for many reasons. First, as already discussed, few general aviation airports are continuously attended or monitored, and doing so is likely to be costly and resource intensive. Second, general aviation airports support a wide variety of operations and consequently must provide limited public access to support and sustain these varied operations including late night cargo operations, training flights, and maintaining adequate numbers of landing facilities that are continuously available for safety in the case of diversions due to weather or mechanical difficulties.

Providing airport access for transient operators also presents a unique security challenge for GA airports, especially during hours when the facility is not attended. However, restricting airports from transient access has significant consequences both for air commerce and for safety. For example, restricting access after hours may impede air commerce and business, especially in remote areas that rely significantly on the presence of a GA airport. Professionals who use GA aircraft to conduct business in these areas may be reluctant to do so if they run the risk of being denied access to the airport because of a late running business meeting that extends beyond the operating hours of the airport, for example. Also, for safety reasons, sufficient numbers of GA airports need to remain accessible, at least for landing aircraft, to provide suitable alternate airports in case of emergency or diversion due to weather.

Supporting airport access during non-attended hours poses significant security challenges. Access control measures must adequately accommodate transient users or the airport runs the risk of becoming inaccessible to certain users. Various options exist for providing both local and transient operators with adequate access to the flight line. For example, at airports implementing access controls to aircraft storage and operations areas, keypad locks can be installed to control access to flight lines. Codes could be provided to transient operators in case they need to access aircraft after hours and could be changed frequently to prevent unauthorized access. Alternatively, more sophisticated access controls can be implemented using key code or card reader systems where transient operators are provided with codes or cards that expire and cannot be used after a certain period.

Display of identification badges in aircraft operations areas may also improve security by identifying those individuals with authorized access to these areas. This can alert observers and security personnel to possible unauthorized access. TSA security guidelines for GA airports suggest that airport identification credentials include features such as a photograph showing a full-face image, the holder's full name, the airport name, employer information, a unique identification number, the

scope of access and movement privileges through easily interpretable means such as color-coding, and a clear expiration date.⁶¹

Pilots, for whom access privileges at multiple airports is needed, require a standardized identification that is easily recognizable at all airport facilities. Presently, FAA certificates do not contain photographs of the certificate holder. However, current regulations require pilots to carry government issued photo identification, such as a driver's licence, and present that identification along with their pilot credentials upon the request of a law enforcement officer or federal official. ATSA (P.L. 107-71) directed the FAA to study ways to improve pilots licenses such as including photos. While the FAA, in response, has taken steps to make newly issued pilot certificates more tamper-resistant and more difficult to forge, many pilots still carry older style paper certificates that can be easily forged. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458, Sec. 4022) requires the FAA to begin issuing improved pilot certificates that include a photograph of the holder and have the capability to accommodate a digital photograph, a biometric identifier, and any other unique identifiers that the FAA may determine to be necessary. While specific plans for issuance of the new pilot certificates with photographs have not yet been announced by the FAA, statutory language provides for the use of designees such as designated pilot medical examiners to issue these new licenses in an effort to "minimize the burdens on pilots."⁶² Advocates for GA pilots have pushed for the use of designated aviation medical examiners for issuance of the new certificates, noting that forcing pilots, particularly pilots in rural areas, to travel to an FAA flight standards district office would be, in their opinion, an unacceptable burden.⁶³

While these new pilot credentials must include the capability to store biometric information, the use of biometrics for identification purposes and access controls in the GA environment introduces many complex technical and policy questions. Implementing biometric access controls at GA airports may be feasible in some cases, but presents significant challenges because of the need to obtain and encode biometric information for transient operators as well as those local tenants, pilots, operators, and airport workers who are authorized to have unescorted access to the flight line.⁶⁴ While biometrics have distinct advantages in terms of logging and tracking access to restricted areas, privacy issues, cost, and logistics may make them difficult to implement effectively in the GA airport environment. However, biometrics may play a more significant role at the GA operator level of security where they could be implemented to control access to operator facilities such as aircraft storage and maintenance hangars. Biometrics may also be used on more limited sets of individuals and integrated into ID card access systems for local aircraft

⁶¹ Transportation Security Administration. *Security Guidelines for General Aviation Airports*.

⁶² P.L. 108-458, Sec. 4022.

⁶³ Aircraft Owners and Pilots Association. *Pilot ID Process Needs to be Convenient, Inexpensive, AOPA Reminds the FAA*. Frederick, MD, July 8, 2005.

⁶⁴ In this context, the flight line refers generally to those areas of an airport where aircraft are accessible including hangars, tie-down areas, and ramps (aprons).

owners, operators, pilots and airport workers. Doing so may allow security efforts to focus more directly on those individuals at an airport that pose more of an unknown threat, such as charter passengers not known to their flight crews and other airport visitors.

Background Checks and Vetting

Because GA airports must maintain a level of reasonable public accessibility to facilitate the freedom of movement by air and air commerce, surveillance, access controls, and physical security measures to protect aircraft and facilities, if needed, must be designed to accommodate a diverse set of legitimate airfield uses. For this reason, implementing access controls and physical security on par with commercial passenger airports is likely to be unrealistic. However, conducting background checks and vetting individuals who routinely access GA airports is seen as a possible technique for assessing potential threats and also as a possible means to focus security resources on conducting surveillance and applying access control measures on visitors who are of an unknown risk.

Vetting of transportation workers and others who routinely access transportation facilities has been a cornerstone of several statutorily mandated projects related to transportation security. For example, the TSA is required to conduct background checks of workers at commercial passenger airports, and the TSA has several ongoing projects, such as the Transportation Worker Identification Credential (TWIC) Program and various airport access control pilot studies, that are attempting to integrate background checks and vetting with the use of biometric access credentials. While it may be some time before these programs reach maturity and can be considered for application in the GA environment, there are already several statutory requirements for vetting GA pilots, pilot applicants, and more recently, prospective aircraft charter and lease customers.

The most widely known of these GA programs is the TSA's alien flight training rule (Title 49, U.S.C. §44939; Title 49 Code of Federal Regulation, Part 1552), which requires the TSA to conduct background investigations of non-U.S. applicants seeking flight training in the United States for aircraft weighing more than 12,500 pounds and requires flight schools or flight instructors to notify the TSA whenever a non-U.S. applicant wishes to initiate flight training in smaller aircraft weighing less than 12,500 pounds. In response to law enforcement and intelligence information revealing that the 9/11 hijackers and accomplice Zacharias Moussaoui received flight training in the United States and amid concerns that foreign terrorists could further infiltrate flight schools in the United States, the Aviation and Transportation Security Act (ATSA, P.L. 107-71) initially placed the Department of Justice in charge of conducting fingerprint-based record checks for alien flight school applicants seeking training to fly aircraft weighing more than 12,500 pounds. Under Vision 100 (P.L. 108-176), this responsibility was moved to the TSA, the process was streamlined to limit the impact of the process on legitimate flight training activities, and reporting requirements were expanded to include a notification requirement whenever foreign flight school applicants initiate flight training in the United States in smaller aircraft weighing less than 12,500 pounds.

A lesser known component of TSA's efforts to vet pilots (whether they be GA pilots, charter pilots, or airline pilots), aircraft mechanics, and dispatchers is the use of threat assessments to screen holders of and applicants for FAA certificates, ratings, or authorizations. Rules pertaining to the security threat assessments for FAA certificate holders and applicants were promulgated on January 24, 2003.⁶⁵ Under these rules, the TSA notifies the FAA whenever a FAA certificate holder or applicant is determined to present a security threat. The FAA, in turn, will deny, suspend, or revoke the individual's FAA certificate as appropriate. While parallel rules were initially issued to carry out security threat assessments for both alien applicants and citizen applicants, the rule pertaining to U.S. citizens was criticized because it lacked adequate safeguards for redress and remedy if FAA certificate actions were taken in response to what the TSA determined to be a security threat. Critics argued that the rule gave the TSA significant power over the issuance of pilot certificates and other aviation credentials without any oversight or redress for the TSA to demonstrate the specific evidence or basis for its decision to identify a certificate holder or applicant as a security threat.⁶⁶ In response to concerns raised regarding the TSA's power over security-related certificate actions and the lack of an adequate redress process, Vision 100 (P.L. 108-176, Sec.601) mandated the TSA to establish a redress and remedy process entitling U.S. citizens subject to certificate action on the basis of a security threat assessment to a formal redress hearing before an administrative law judge and an appeals process before a panel convened by the Transportation Security Oversight Board. The TSA has not yet issued revised rulemaking to conform with the statutory requirements set forth in Vision 100, and therefore, existing regulations to enforce FAA certificate actions on the basis of security threat assessments no longer apply to U.S. citizens.⁶⁷ However, security threat assessments for alien FAA certificate holders and applicants remains unchanged.

Although security threat assessments for citizen pilots, mechanics and other FAA certificate holders and applicants has been suspended until the TSA develops a process and issues rulemaking to conform with statutory requirements for redress and remedy, regulations still require fingerprint-based criminal history records checks for charter pilots who fly aircraft weighing more than 12,500 pounds.⁶⁸ However, other GA pilots – who make up the majority of the more than 600,000 active pilots in the United States – are not required to submit to any formal background screening or checks. Some critics of background checks and vetting maintain that they are costly and an unnecessary intrusion into the privacy of citizens. On a pragmatic level, some question whether background checks for GA are needed at all, particularly at small, rural airports where pilots, ramp workers, and others who

⁶⁵ Transportation Security Administration. "Threat Assessment Regarding Citizens of the United States and Alien Holders Who Hold or Apply for FAA Certificates; Final Rules." *Federal Register*, 68(16), pp. 3756-3769 (January 24, 2003).

⁶⁶ See, e.g., Llewellyn King, "Adm. Loy, You Know Better: Rescind This Rule." *White House Weekly*, 24(10), March 11, 2003, 1-2.

⁶⁷ Transportation Security Administration. Memorandum to the Dockets from Pamela Hamilton, Director of Aviation Initiatives Regarding TSA Rulemaking Docket No. TSA-2002-13732 and TSA Rulemaking Docket No. TSA-2002-13733. March 16, 2004.

⁶⁸ Title 14 CFR §1544.101 and §1544.230.

frequent the airport are largely known to each other. Nevertheless, background checks and other vetting activities have been looked upon favorably by policymakers as a core component of a layered security system and could be further expanded in their application to GA operators.

One area where background checks and security threat assessments is being incorporated into GA operations is for the vetting of prospective charter and lease customers. Under statutory provisions set forth in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458, Sec. 4012), the TSA is charged with the task of setting up a mechanism for charter and aircraft lease operators to voluntarily submit the names of prospective clients seeking access to aircraft weighing more than 12,500 pounds for screening against the consolidated terrorist watch list. Aircraft operators may deny individuals access to aircraft if their name is found to match watch list records. While the legislative language limited the applicability of this vetting procedure to aircraft weighing more than 12,500 pounds, the feasibility of extending this capability to charters and leases of smaller aircraft, based on the initial experience with larger aircraft, was debated during consideration of this legislation. While terrorist database screening of prospective charter and lease customers as legislated is voluntary, policymakers may also consider whether mandatory screening of aircraft charter and lease customers is warranted. However, because the capability to screen names against terrorist watch list information is tied to the functionality of the controversial Secure Flight program for prescreening airline passengers, implementation of a charter and lease customer prescreening mechanism – which is currently not operational – may be further delayed by ongoing difficulties in meeting congressionally mandated safeguards for data and privacy protections and redress and remedy for aggrieved individuals who are erroneously identified as suspected or known terrorists.⁶⁹ Presently, language in the FY2006 Department of Homeland Security Appropriations Act (P.L. 109-90) prohibits full-scale deployment of the Secure Flight system until the GAO certifies that these lingering concerns are adequately addressed.

Besides prospective charter and lease customers, the screening of prospective aircraft purchasers can serve as an important deterrent to prevent terrorists or organizations that support terrorism from acquiring aircraft that could be used in a terrorist attack. Under Department of the Treasury regulations, promulgated to meet requirements of the USA PATRIOT Act (P.L. 107-56), aircraft sales must comply with various information sharing, reporting, and records keeping requirements aimed at identifying suspicious transactions and preventing money laundering.⁷⁰ However, because many other large-scale financial transactions such as the sale of houses, boats, and cars must be similarly reported, the volume of transactions may make it difficult to quickly identify suspicious aircraft transactions. The main intent of these regulations is to spot potential attempts to launder illegal funds in support of terrorist or criminal activities, and therefore the regulations are not specifically designed to vet purchasers of GA aircraft against terrorist watch lists. The capability to detect

⁶⁹ See CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, by Bart Elias, William Krouse, and Ed Rappaport.

⁷⁰ See Title 31 Code of Federal Regulations, Part 103.

aircraft sales to suspected terrorists or their associates and vet aircraft purchasers against terrorist watch lists under these reporting requirements remains unclear.

Physical Security Measures for Airports

Other than surveillance, access controls, and background checks, there are a variety of other options for enhancing the general physical security of airport facilities. One of the most obvious of these measures is erecting physical barriers, such as chain-link perimeter fencing, around security sensitive locations on the airfield. However, the TSA cautions that while physical barriers such as fencing, walls, electronic boundaries, and even natural barriers can protect airport areas from unauthorized access, these methods by themselves will not prevent determined intruders from gaining access. The TSA further notes that excessive spending on extensive perimeter enhancements may actually be detrimental to an airport's overall security posture to the extent that these efforts take away from opportunities to improve upon other aspects of security.⁷¹ Besides fencing, protective lighting can often serve as an effective deterrent against theft, vandalism, unauthorized access, and other illegal activity at night.⁷²

While various combinations of physical barriers and lighting may deter unauthorized access at airports, the TSA notes that storing aircraft in hangars provides one of the most effective method of securing GA aircraft.⁷³ However, at many GA airports, hangar space is in short supply and the demand for hangars make them very costly, especially for some small, privately owned aircraft. Language in the Century of Aviation Reauthorization Act – Vision 100 (P.L. 108-176, Sec. 149) provides greater flexibility in the allocation of federal Airport Improvement Program (AIP) funds for the construction of hangars at GA airports. Also, to foster private investment in hangar construction, additional language in Vision 100 (P.L. 108-176, Sec. 165) provides assurances for long-term lease agreements between tenant aircraft owners who build hangars using their own funds and airport operators.

Physical Security Measures for Aircraft

While surveillance, access controls, and physical security measures at airports can provide effective deterrents, these measures may be costly and challenging to implement at many GA airports, especially smaller airports. Measures to physically secure aircraft can be viewed as either an additional layer of security to prevent theft and unauthorized access to aircraft at airports with extensive surveillance and access controls or as a primary means of security at some airports with more limited security capabilities.

Physical security measures for aircraft may include cabin and ignition locks that may already exist for certain aircraft as well as supplemental immobilizing devices

⁷¹ Transportation Security Administration. *Security Guidelines for General Aviation Airports*.

⁷² *Ibid.*

⁷³ *Ibid.*

such as propeller, throttle, control surface, and tie-down locks. The TSA's *Security Guidelines for General Aviation Airports* recommends storing aircraft in locked hangars, consistent use of aircraft door locks, using keyed ignitions when appropriate, and not leaving keys in aircraft as some basic steps to secure GA aircraft. The guidelines also recommend using an auxiliary lock such as commercially available propeller, throttle, or tie down locks to further protect GA aircraft. The TSA suggests that "[p]ilots should employ multiple methods of securing their aircraft to make it as difficult as possible for an unauthorized person to gain access to it." However, it is apparent that this common sense advice is not always heeded. In the October 2005, theft of a Cessna Citation VII business jet, it was reported that the aircraft – which does not need a key to start – was left unlocked.⁷⁴

While building or renting secured hangar space may be cost prohibitive to many light aircraft owners, locks and other security devices may provide a common sense, cost effective means to reduce the vulnerability of GA aircraft to theft. Given that aircraft are high value assets, locks may offer a relatively low-cost means to reduce vulnerability. Purchasing and installing secondary locks could benefit aircraft owners and operators by providing added protection against theft and unauthorized access.

In the absence of explicit federal standards or requirements, some states have taken initiatives to require specific actions for securing GA aircraft. New Jersey, for example, has implemented a state-wide "two-lock rule" requiring any aircraft parked or stored at a GA facility within the state for more than 24 hours to either secure the aircraft with two distinct locking devices or disable the aircraft in a manner to prevent theft or illegal use.⁷⁵ The Strengthen Aviation Security Act (H.R. 2649) would require airport operators to ensure that "...all general aviation aircraft, while parked at such airports, are secured by a visible immobilizing device (such as a prop lock)." Propeller locks and throttle locks may provide relative low cost, relatively effective deterrents to unauthorized use and theft of aircraft.

Securing Agricultural Aviation Operations

The specific intelligence and law enforcement evidence pointing to al Qaeda's interest in crop dusting aircraft in the months leading up to 9/11 suggests that the agricultural sector of general aviation should be particularly alert to suspicious activities. Because agricultural aviation operations largely take place in rural environments, away from highly populated areas, increased awareness of this threat coupled with operators increasing their vigilance and taking steps to secure their aircraft may serve as an adequate deterrent. However, the unique capabilities of aircraft, both airplanes and helicopters, used in aerial application make them specifically attractive to terrorists. For this reason, the TSA recommended to operators of agricultural aircraft that they use multiple security devices – such as throttle and control locks, propeller locks, and hidden ignition switches – to secure aircraft, store aircraft in hangars with electronic security systems and steel doors, and

⁷⁴ Mike Morris. "Buford Man, 22, Accused of Stealing Jet."

⁷⁵ U.S. Government Accountability Office. *General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector Is Critical to Long-Term Success*. GAO-05-144, November 2004.

when hangars are not available, park heavy equipment in a manner to prevent the movement of aircraft.⁷⁶ The National Agricultural Aviation Association has provided additional guidance to operators of agricultural aircraft advising them to: secure pesticide storage areas; implement procedures for the shipping and receiving of chemicals; secure facilities and limit access; post security signs; improve lighting of storage areas; secure fences and gates; conduct security inspections to check for signs of intrusion or tampering; maintain logs to track visitor access to facilities; coordinate with local law enforcement and fire departments; and develop site security plans as required to comply with HAZMAT regulations.⁷⁷

Flight School Security

Besides agricultural aircraft operations, another sector of GA flying that has raised security concerns has been flight schools. Flight schools have been spotlighted, in large part, because of intense media coverage of the apparent relative ease that some of the 9/11 hijackers were able to obtain flight training in the United States, and the reported lack of safeguards to prevent incidents like the intentional crash of a small single-engine airplane into a downtown Tampa, Florida building piloted by a student pilot who stole the aircraft while conducting an unsupervised pre-flight inspection.⁷⁸

To address lingering concerns over flight school security, Vision 100 (P.L. 108-176) requires specific flight school security awareness training for all flight school employees. To meet this statutory requirement, the TSA has developed a standardized computer-based flight school security awareness training program, although flight schools have the option of developing their own security training program that must obtain TSA approval. New hires must receive initial security awareness training within 60 days of employment, and employees must complete annual recurrent training in security awareness. The training indoctrinates flight school employees on fundamentals of security awareness, security practices, and appropriate responses to suspicious events. In addition to the statutory requirement for security awareness training, the TSA has issued several recommendations for flight schools in its security guidelines for GA airports.⁷⁹ These recommendations largely focus on increasing surveillance and supervision of students and renter pilots and better controlling access to aircraft and aircraft keys. Other steps that may be taken by flight schools to improve security include background checks of prospective employees, particularly prospective flight instructors and maintenance personnel; establishment of formal written security procedures for employees and customers;

⁷⁶ Transportation Security Administration. *Security Guidelines for General Aviation Airports*.

⁷⁷ Regulatory Consultants, Inc. "Secure Your Operation Today." *Agricultural Aviation*, July/August 2005, 17-18.

⁷⁸ Jean Heller and Alicia Caldwell. "Flight Schools: Breach of Trust Difficult to Prevent." *St. Petersburg Times*, January 8, 2002.

⁷⁹ Transportation Security Administration. *Security Guidelines for General Aviation Airports*.

display of identification by employees; and various access controls and surveillance measures for the flight line.

Security Best Practices for Business and Charter Aviation

In addition to agricultural aviation and flight schools, another sector of GA with unique security needs is business aviation. Larger, faster business jets introduce unique security concerns because of their size and speed as well as their relatively high value and, in some instances, the prominence of passengers carried on board these aircraft. While business jets make up a relatively small percentage of general aviation aircraft, their larger size, heavier payload, and faster speed introduce unique risks. Chartered business jets and turboprops also pose a unique risk because, unlike corporate or privately owned aircraft, flight crews often do not know their passengers.

In coordination with the TSA, the National Business Aviation Association has implemented a program promoting aviation security best practices among business aircraft operators.⁸⁰ The program focuses on various facets of operator security including identifying security roles within an operator's organization; providing security training to flight department personnel; establishing sound physical security measures to control access to facilities and aircraft; issuing photo IDs for crew members; conducting pre-flight security inspections of aircraft; matching baggage to passengers; maintaining positive control of baggage; and developing and keeping up to date site specific security and emergency response plans.

The TSA Access Certificate Program. Based in part on the NBAA's initiatives regarding aviation security best practices, the TSA initiated a pilot program for implementing security protocols for business aircraft operators in the spring of 2003. The program, dubbed TSAAC for TSA Access Certificate, is currently being implemented on a trial, proof-of-concept basis at select airports on the east coast. Corporate aircraft operators that implement TSA-approved security programs under TSAAC are currently granted unimpeded access to international airspace, whereas other operators must currently enter and depart U.S. airspace through one of eight designated "portal" countries.⁸¹ The TSAAC program was initially offered as a pilot program to operators based at Teterboro Airport (TEB) in New Jersey. The program has since been expanded to include operators at Westchester County Airport (HPN) in New York, and Morristown Airport (MMU) in New Jersey. While the specifics of the TSAAC program are regarded as security sensitive information, the program generally requires operators to implement security procedures similar to the operational security measures required for charter aircraft operators who fly aircraft weighing more than 12,500 pounds. Elements of the program include various aspects of physical security measures for aircraft, vetting of customers and other visitors, control of passengers and baggage, access controls for the flight line and aircraft operations areas, and the utilization of threat intelligence.

⁸⁰ National Business Aviation Association. *NBAA Best Practices for Business Aviation Security*. Washington, DC: National Business Aviation Association, Inc.

⁸¹ David Esler. "TSAAC: Business Aviation's New Ticket to Enter?" *Business & Commercial Aviation*, May 2003, pp. 200-210.

The TSAAC is regarded by many in the industry as being a means for business aircraft operators to gain "...equal access to airspace and airports as currently given to scheduled air carriers."⁸² This may include access to various flight restricted areas throughout the United States. While the TSAAC has been hailed by the business aircraft industry as a potential model for broader security initiatives covering the business aircraft sector of GA, the program has been slow to evolve and is still limited in its scope of applicability. While it was announced on December 30, 2004 that the TSAAC program would be further expanded to additional airports⁸³, progress to evaluate and identify additional benefits of the program have slowed. Report language submitted by the House Committee on Appropriations (H.Rept. 109-241; P.L. 109-90) signaled strong support for the TSAAC program, encouraging the TSA to move forward with the program during FY2006.

Access to Ronald Reagan Washington National Airport. TSAAC has been regarded by many in the business aviation community as a model for granting business aircraft operators access to restricted airspace. Toward that objective, the TSAAC served as an important starting point for implementing regulations allowing GA flights to resume at the Ronald Reagan Washington National Airport (DCA) as mandated under Vision 100 (P.L. 108-176). Because DCA is in such close proximity to Washington, DC, it had generally been off limits to GA operators since the terrorist attacks of September 11, 2001. However, on August 18, 2005, DCA reopened to GA operators on a very limited basis under an interim final rule detailing extensive security requirements for GA operators to gain access to the airport.⁸⁴ In addition to adhering to security protocols similar to those outlined in the TSAAC program, operators wishing to fly to and from DCA must: have their flight crews cleared by background checks; submit passenger and crew member names for vetting against terrorist watch lists; submit to physical screening of passengers, crew members, and baggage; transition into DCA from one of 12 designated gateway airports; and post designated armed security officers on each flight to and from DCA. Operators must reimburse the TSA for the direct costs associated with these security measures which in effect makes access to DCA cost prohibitive for most GA operators. As currently implemented, the security provisions for access to DCA are designed primarily to accommodate larger charter operators and high-end corporate aircraft. The program is not currently available to privately-owned aircraft, but the TSA indicated that the program may be expanded in about one year based on the initial experience with charter and corporate operators.⁸⁵

⁸² National Business Aviation Association. *TSA Access Certificate (TSAAC)* – Updated December 23, 2003. Washington, DC: National Business Aviation Association, Inc.

⁸³ Transportation Security Administration. *TSA and National Business Aviation Association to Expand General Aviation Security Partnership Program*. Press Release, December 30, 2004.

⁸⁴ Transportation Security Administration. Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations; Interim Final Rule. *Federal Register*, 70(137), 41586-41603 (July 19, 2005).

⁸⁵ See CRS Report RS22234, *Protecting Airspace in the National Capital Region*, by Bart Elias.

Security Measures for Charter Operations. While corporate and privately owned aircraft primarily deal with passengers known to the pilots and operators, passenger charter aircraft present unique security challenges because customers are sometimes unknown or unfamiliar. Charter aircraft weighing more than 12,500 pounds maximum takeoff weight must adhere to specific security regulations referred to as the *twelve-five* security program in reference to the aircraft weight criteria.⁸⁶ Twelve-five security program requirements include passenger identification checks, fingerprint-based criminal history records checks for flight crew members, application of specific bomb and hijacking notification procedures and requirements, and implementation of a TSA-approved operator security program. Each operator must designate a security coordinator within the organization, provide training and information to employees with security-related duties, and have procedures in place to coordinate with law enforcement entities responding to security threats. Although cockpit doors are not a requirement for twelve-five operations, if an aircraft has a cockpit door, procedures must be in place to restrict access to the flight deck.

In addition to these requirements of the twelve-five security program, operators of passenger charter flights in aircraft weighing more than 100,300 pounds maximum gross weight or and aircraft with 61 or more passenger seats must implement additional security measures laid out in the TSA's private charter program, including a requirement for physical screening of passengers and accessible baggage.⁸⁷ Also, regardless of aircraft weight, if a passenger-carrying charter flight loads or unloads passengers at a designated sterile area of a commercial airport (that is, beyond the security screening checkpoint), that operation must also adopt the private charter security program. The private charter program prohibits passengers from carrying weapons, explosives, and incendiary devices, and requires that metal detectors and x-ray systems used in the screening of charter passengers meet standards established by the TSA. However, physical screening of passengers can be conducted by TSA-approved private screeners and is not typically carried out by federal screeners unless arrangements are made to enplane and deplane from the sterile area of commercial airports. Private charter operators of these larger aircraft must establish procedures to prevent unauthorized access to aircraft and other access controlled areas as specified in the operator's security program and must carry out a security inspection of aircraft whenever access control measures, such as posted security guards or adequate access controls to aircraft, are not maintained. In addition to flight crew members, other employees of private charter operating large aircraft that have unescorted access to aircraft and secured areas must submit to fingerprint-based criminal history records checks, and security coordinators and crew members must complete annual recurrent security training.

While the twelve-five and private charter security regulations specifically apply to charter operations, the TSA requires GA operators authorized to enplane or deplane into the sterile area of commercial passenger airports to conduct TSA-approved physical screening of passengers, flight crew members, and their carry on

⁸⁶ See Title 49, Code of Federal Regulations, §1544.101(e).

⁸⁷ See Title 49, Code of Federal Regulations, §1544.101(b) and (f).

items.⁸⁸ While these regulations are in place to make allowances for certain GA operations that might be permitted to enplane and deplane at sterile airport areas while preventing the introduction of weapons, explosives, or incendiary devices into the commercial passenger aircraft environment, corporate and privately owned GA aircraft are rarely granted access to sterile areas. Also, while the required adoption of a twelve-five security program is only required of charter operators, regulations stipulate that GA operators of aircraft weighing more than 12,500 pounds maximum takeoff weight could be required to conduct preflight security searches and screen passengers, crew members, and carry-on items before boarding in accordance with security procedures approved by TSA if notified to do so by the TSA.⁸⁹ While these security measures have never been implemented, they could become effective upon notification to operators through means such as the Notices to Airman (NOTAM) system and may be carried out, for example, upon receipt of specific, credible intelligence suggesting a terrorist plot to hijack business jets.

Airspace Restrictions

Besides efforts to tighten security at GA airports and vet pilots, GA security measures have focused extensively on imposing flight restrictions over various potential terrorist targets. These security-related flight restrictions have been highly contentious because: they have a direct impact on air commerce and the freedom of movement by air; the potential for airspace violations has significant repercussions for both professional and private pilots; surveillance, airspace protection, and enforcement of airspace restrictions can be costly and resource intensive; and these measures are considered by many to be of questionable effectiveness.

Airspace Restrictions Around Washington, DC. While many low-altitude flight restrictions around sensitive locations for reasons of national security have long been in place, the number and scope of these restrictions has expanded significantly since the terrorist attacks of September 11, 2001. The most comprehensive of these restricted areas is the airspace around Washington, DC, which consists of a Flight Restricted Zone (FRZ), 15-nautical miles in radius, and a larger area – referred to as the Washington, DC Air Defense Identification Zone (ADIZ)⁹⁰ – where flights must adhere to specific flight plans and air traffic communications and surveillance requirements. An FAA proposal⁹¹ to make the airspace restrictions around Washington, DC permanent has met with considerable disapproval from pilots and GA advocacy groups who had hoped these restrictions

⁸⁸ See Title 49, Code of Federal Regulations, §1550.5.

⁸⁹ See Title 49, Code of Federal Regulations, §1550.7.

⁹⁰ The term Air Defense Identification Zone (ADIZ) has long been in place and refers to any area of airspace where the identification, location, and control of aircraft are required in the interest of national security. Prior to September 11, 2001, this term generally referred to buffer zones around coastal waters and international borders of the United States. Since September 11, 2001, the ADIZ concept has been expanded to include zones within the United States such as in the vicinity of Washington, DC.

⁹¹ Federal Aviation Administration. “Washington, DC Metropolitan Area Special Flight Rules Area; Proposed Rule.” *Federal Register*, 70(149), 45250-45261 (August 4, 2005).

would be eased. Presently, the airspace restrictions continue to exist as temporary flight restrictions (TFRs) while the decision to make them permanent remains under review. A detailed discussion of the airspace restrictions in the Washington, DC area can be found in CRS Report RS22234, *Homeland Security: Protecting Airspace in the National Capital Region*, by Bart Elias.

Security-Related Flight Restrictions Throughout the United States.

Other than the airspace restrictions around Washington, DC, various security-related flight restrictions have been put in place to protect national security interests and ostensibly to protect potential high-profile terrorist targets from aerial attacks. At various times since September 11, 2001, flight restrictions have been imposed to protect airspace around major U.S. cities and other potential terrorist targets. For example, during the build up toward the war in Iraq in early 2003, additional airspace restrictions were put in place around New York City, Chicago, and Disney theme parks in addition to establishing the ADIZ around Washington, DC to augment the FRZ that had already been put in place following the terrorist attacks of September 11, 2001. Flight restrictions around major cities besides Washington, DC were lifted, but have been reinstated for brief periods during times when the national security threat level has been elevated or when special events warranted the establishment of temporary flight restrictions. However, the flight restrictions around Disney theme parks have continuously remained in effect and are now mandated in statute. In addition to these restrictions, the Consolidated Appropriations Act of 2004 (P.L. 108-199, Sec. 521) establishes permanent flight restrictions over stadiums and motor speedways during major league baseball games, national football league and National Collegiate Athletic Association (NCAA) division I football games, and major auto racing events. These flight restrictions establish a three nautical mile radius around the effected facility extending from the surface to 3,000 feet. GA aircraft are generally prohibited from this airspace, but exceptions may be made for flight operations directly related to the sporting event, broadcast coverage of the sporting event, or to provide safety and security for the event. Exceptions may also be made in cases where the venue is in close proximity to an airport, in which case aircraft may enter into the restricted area if necessary to land or takeoff from the airport using standard air traffic procedures. These restrictions have been criticized by some because they are selective in the events that are covered by the statutory mandate and therefore do not encompass all large-scale outdoor assemblies. The restrictions have also been criticized because the relatively small size of restricted airspace, while often interfering with flight operations, is considered by many to provide an inadequate perimeter for establishing adequate airspace protections to the sites they are intended to protect.

Presidential Airspace Restrictions. In addition to the stadium and theme park overflight rules, the temporary flight restricted areas put in place around sites visited by the President are particularly troublesome for many pilots. Unlike the stadium and Disney theme park areas which encompass a relatively small footprint, the flight restrictions put in place for presidential visits encompass a much wider area. The area of these restrictions has grown from a 3-mile radius extending 3,000 feet in altitude before 9/11, to a 30-nautical mile radius reaching up to 18,000 feet in altitude. This effectively increased the footprint of the restricted airspace around the President from just over 28 square miles to more than 2800 square miles, and increased the cubic volume of protected airspace around the President by 600%.

Typically, during a presidential visit, GA flights are completely prohibited within 10-nautical miles of the designated site. Between 10 and 30 nautical miles from the designated site, flights below 18,000 feet must be on active flight plans and in constant communication with air traffic controllers.

The fact that these airspace restrictions to protect the President are often put in place with little advance notice has the potential of catching pilots off guard. Because these presidential movement temporary flight restrictions (TFRs) change dynamically with the President's schedule, pilots can be easily misinformed or confused about the specific location of the restricted airspace and the effective times of the restrictions, which usually includes a block of time around the President's expected presence but can change on short notice. Also, these restrictions are often defined in terms that may not be meaningful to GA pilots whose aircraft may lack the navigational capability to identify the boundaries of restricted areas. The FAA and user groups such as AOPA have worked to increase pilot awareness regarding the movements of the President and provide pilots with up to date information regarding presidential movement TFRs including graphical depictions of affected airspace. Nevertheless, identifying these airspace boundaries continues to be a challenge, particularly to pilots flying primarily by visual means and relying on landmarks on the ground to avoid airspace incursions. The AOPA and other GA advocacy groups have questioned the need for restrictions over such a wide area and have lobbied to keep the impacts of these security measures on airspace accessibility to a minimum.⁹²

Policy Issues Regarding Airspace Restrictions. Besides these specific objections to security-related flight restrictions, many aviation interests and homeland security specialists have raised broader policy questions about the effectiveness of these various airspace restrictions and special operating procedures, noting that enforcing airspace restrictions is costly and resource intensive and providing protection to defend sites against aerial attacks is an even greater challenge. The resource requirements and associated costs for monitoring restricted airspace and providing airspace protection around critical sites raise policy questions regarding the appropriate balancing of these measures with efforts to address other homeland security threats, and the effect of these measures on air commerce and the freedom of movement by air.

Surveillance and Monitoring of Restricted Airspace. Surveillance and monitoring capabilities present a significant challenge for protecting airspace. This is, in part, because detailed information on specific GA aircraft is not provided to air traffic controllers and airspace monitors unless the aircraft is transmitting a unique identifying code to air traffic radar sites. Under the current radar system, providing GA aircraft with unique identifiers and tracking all GA aircraft could, at times, prove overwhelming for air traffic controllers. Under present day air traffic control procedures, pilots must file flight plans, receive unique identifier codes to transmit, and make radio calls to air traffic controllers to establish "radar contact" allowing controllers to identify and track a specific flight. Under normal circumstances in clear weather, many flights never file a flight plan nor contact air traffic controllers

⁹² See, e.g., Aircraft Owners and Pilots Association. *Members of Congress Join AOPA Outcry Over Presidential Movement TFRs*. Frederick, MD; May 16, 2003.

because they are not required to do so. But, to operate inside certain restricted airspace like the Washington, DC ADIZ, pilots must follow the aforementioned procedures for filing flight plans, transmitting unique identifying codes, and communicating with air traffic controllers – procedures that are often workload intensive for both pilots and controllers. Technologies may provide a solution that could ease pilot and controller workload associated with these transactions. For example, Mode S transponders are capable of automatically relaying detailed aircraft identifier information to air traffic radars, but most smaller GA aircraft do not have this technology and it is expensive to install. Similarly, emerging technology called Automated Dependent Surveillance - Broadcast (ADS-B) can transmit detailed aircraft information to ground stations and other aircraft, but this new technology is only beginning to become available and surveillance capability is not yet available in all parts of the United States. While ADS-B shows significant promise for improving safety as well as security, the FAA is still reviewing its investment strategy in this technology. In the meantime, surveillance of GA aircraft must rely on current radar capabilities, involving close coordination between pilots and air traffic controllers. This imposes additional workload on both pilots and controllers. This increased workload has a direct bearing on FAA resources. For example, the FAA estimates that making the Air Defense Identification Zone (ADIZ) around Washington, DC permanent will cost about \$11 million per year, mostly linked to increased labor costs associated with processing flight plans and providing air traffic services to aircraft operating under visual flight rules (VFR) that would otherwise present little or no impact on the air traffic control system.⁹³

Airspace Protection and Homeland Defense. Besides the resources and costs associated with monitoring flights, the capability to establish formidable airspace protections in restricted airspace is a central issue for homeland security. The effectiveness of airspace protections and interagency coordination in providing homeland security and defense is at the crux of the policy debate over effective airspace security. This is because airspace restrictions by themselves are not particularly useful tools unless a coordinated response to protect critical assets within those protected areas are effective. Merely relying on enforcement tools is not likely to be of significant benefit because terrorists are likely to care little that they are violating airspace restrictions in carrying out an attack.

The North American Aerospace Defense Command's (NORAD's) Operation Noble Eagle is charged with the task of interdicting aircraft believed to pose a national security risk. Since September 11, 2001, fighter jets have scrambled to respond to almost 2,000 domestic air security events.⁹⁴ While these incidents include escorts of international passenger airliners where passengers names matched information in terrorist databases, the large majority of these interdictions involved

⁹³ Aircraft operating under VFR may, on occasion, request traffic advisories or “flight following” from air traffic controllers on a workload-permitting basis. However, except for regulations established for security monitoring purposes, VFR aircraft are not required to interact with air traffic services unless flying in specially designated airspace near towered airports or above 18,000 feet.

⁹⁴ First Air Force. *Operation Noble Eagle: Defending America's Skies*. Tyndall Air Force Base, FL.

intercepts of small GA aircraft that strayed into restricted or prohibited airspace. In the environment of heightened security since the 9/11 attacks, the FAA, NORAD, and aviation user groups such as the AOPA and the NBAA have made extensive efforts to heighten pilots' awareness regarding airspace restrictions and proper procedures to follow if intercepted by DHS, law enforcement, or military aircraft.

Despite these intensified efforts to protect major metropolitan areas and critical sites from aerial attacks, it has been reported that military officials have concluded that stopping a 9/11-style attack would be difficult unless fighter jets were already airborne.⁹⁵ Maintaining a constant airborne defense presence, however, would be extremely costly and resource intensive. Ground-to-air missiles have been deployed around Washington, DC, but are largely seen as a measure of last resort for protecting a limited number of key locations against an aerial attack, whether that attack involves a GA aircraft or a commercial airliner.⁹⁶

Because of the continuing challenges in providing effective national airspace defenses, the adequacy of airspace protection initiatives will likely depend on close cooperation and coordination between the FAA, the DHS, and the DoD as well as effective command and control within each of these organizations. Presently, event response is coordinated through the FAA's Domestic Events Network (DEN), a continuously operated unclassified network for sharing critical incident information regarding aircraft deviations and violations of security restricted airspace, and the TSA's Transportation Security Operations Center (TSOC), the central hub for exchanging information regarding aviation threats located in Herndon, VA. The function of these facilities is to provide a shared situational awareness of aviation threats including, but not limited to, threats posed by GA aircraft. Besides the TSA, NORAD, and the FAA, other key agencies involved in airspace surveillance and protection include Customs and Border Protection (CBP) and the Coast Guard which provide air interdiction and situation response within the DHS as well as the Federal Bureau of Investigation (FBI).⁹⁷ These agencies also coordinate with federal, state, and local law enforcement to integrate threat response.

Coordinated threat response was observed in the May 11, 2005 event where an errant small private airplane penetrated deep into the FRZ around Washington, DC. The coordinated response to this threat included deployment of fighter jets, helicopters from CBP, and federal and state law enforcement assets to interdict and intercept the aircraft. While the response to this perceived threat was by most accounts well coordinated, concerns have been raised that response to a more formidable threat, such as a faster moving aircraft attempting to evade airspace protections and defenses may be much more difficult to interdict and may require a carefully orchestrated response involving close coordination between responsible agencies. While these agencies continue to assess and refine their monitoring and

⁹⁵ Associated Press. "Intercept Tests Show U.S. Air Vulnerability." January 15, 2004.

⁹⁶ Statement by Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense before the Committee on Government Reform, United States House of Representatives, July 21, 2005.

⁹⁷ *Ibid.*

response capabilities, Congress may continue to conduct oversight of interagency coordination to ascertain whether there is an adequate level of preparedness to deal with airborne threats, including threats posed by GA aircraft, and assess whether steps taken to protect critical assets from aerial attacks do not unduly burden GA operators or compromise flight safety. While the focus to date has been airspace protection in and around Washington, DC, Congress may also examine whether the capability and coordination between federal, state, and local agencies to monitor and protect airspace in other areas of the country is adequate and appropriately balances homeland security needs with air commerce and aviation safety concerns.

Related Legislative Actions in the 109th Congress

GA security has been a topic of continued legislative interest in the 109th Congress. Based on a Senate-passed amendment introduced by Senator Clinton (S.Amdt. 1106 to H.R. 2360), conference report language in the FY2006 DHS Appropriations Act (P.L. 109-90) requires the DHS, in coordination with the Department of Transportation, to “...study the vulnerability posed to high-risk areas and facilities from general aviation aircraft that could be stolen or used as a weapon against those areas.” Areas to be considered in the assessment include critical transportation infrastructure, nuclear facilities, military bases, and highly populated areas with similarly situated critical infrastructure. The analysis is to identify vulnerabilities at GA airports, the sufficiency of existing security measures, and any additional security measures that could be implemented.

Additional legislation introduced in the House would focus on site-specific measures to improve security at GA airports. The Strengthen Aviation Security Act (H.R. 2649), introduced by Representative Markey on May 26, 2005, would require airport operators to develop site-specific vulnerability assessments for each GA airport and develop a plan for addressing vulnerabilities identified within one year of enactment. H.R. 2649 would also require background checks and terrorist database screening for any individuals with access to general aviation aircraft. While the bill language, in its broadest interpretation, could apply to just about anyone who would have occasion to visit or transit through a general aviation airport, the intent appears to be focused on airport workers and pilots to parallel requirements for unescorted access to secured areas of commercial airports. The bill would also require all GA aircraft to be secured by visible immobilizing devices such as prop locks while parked at GA airports.

In addition to these measures, H.R. 2649 calls for establishing no-fly zones during periods of high terrorist threat levels and any other applicable times identified by the DHS around all sensitive nuclear facilities, chemical facilities where a release of hazardous materials could endanger one million or more lives, and any other facilities designated by the Secretary of Homeland Security.

On July 21, 2005, Representative Sweeney introduced the General Aviation Security Act of 2005 (H.R. 3397). This bill would require all operators of public- and private-use airports in the United States to register with the DHS and undergo a registration renewal process every three years. The proposed registration process

would include a security plan documenting site-specific security procedures consistent with the TSA's most recent security guidelines for GA airports. In developing security plans, operators would be required to provide a written description of how the airport has addressed each recommendation or justify why a particular recommendation was not adopted. The legislation calls for using self-assessment tools to identify airport characteristics for security purposes in the development of airport-specific security plans. In addition to providing security plans to the DHS as part of the registration process, airports would also be required to submit their security plans to local law enforcement agencies having jurisdiction over the airport.

H.R. 3397 would also require that all public-use airports:

- Ensure that all aircraft crews verify the identity of all aircraft passengers;
- Maintain logs of all transient aircraft for a minimum of five years;
- Make a list of emergency telephone contacts available to all airport personnel;
- Restrict the access of unlicensed individuals and student pilots to aircraft keys;
- Require aircraft renters to present government-issued identification in addition to their pilot's license;
- Post applicable security warning signs and advisories where appropriate;
- Provide emergency responders with confidential emergency locator maps of the airport identifying items such as runways, ramp areas, fence lines, and gates; and
- Familiarize local law enforcement with the airport and consult with them in developing security procedures.

Additionally, at all GA airports – both public- and private-use – all aircraft would be required to be double-locked with one external lock and one lock inside the aircraft. Also, at all GA airports, hangars would be required to be locked when not in use and adequate fencing would be required for secure areas.

Besides these more comprehensive measures addressing GA security, concerns over airspace violations that complicate the task of protecting critical assets from aerial attack have prompted the introduction of legislation calling for stiffer fines for airspace violators and mandatory pilot training on airspace restrictions. In response to concerns over frequent violations of restricted airspace near Washington, DC, Representative Blunt introduced the Capitol Airspace Enforcement Act (H.R. 3465). The bill calls for civil penalties ranging from \$10,000 up to \$100,000 for violations of the 15-mile radius flight restricted zone (FRZ) around Washington, DC, and fines of up to \$5,000 for violations of security protocols while operating in the larger air defense identification zone (ADIZ). The measure also includes a requirement for mandatory pilot training regarding the airspace restrictions and proper operating procedures and compliance with airspace restrictions.

While GA advocacy groups like the AOPA and the NBAA support mandatory education for pilots flying in and near restricted airspace and have taken considerable

steps on their own initiative to provide educational materials regarding the airspace restrictions, they strongly oppose stricter penalties and believe that administrative actions and fines already available to the FAA along with the potential threat of a shoot down already serve as sufficient deterrents for inadvertent airspace violations.⁹⁸ These groups have voiced significant concerns over the impact of airspace restrictions and homeland security regulations on air commerce and the freedom of movement by air. These groups have also opposed comprehensive legislative measures, such as H.R. 3397, that mandate broad security requirements over the wide range of GA airports and operations cautioning that imposing such mandates "...would be ridiculously expensive, is unnecessary, and ignores the guiding principle of making investments in security based on risk."⁹⁹ In response to this criticism, attempting to tailor homeland security policy to fit the risk posed by widely varied GA operations, allocating budgets and resources to address security priorities, and addressing concerns about potentially impeding air commerce or compromising aviation safety are likely to remain ongoing challenges for the Congress.

⁹⁸ Spencer S. Hsu. "Bill Targets Errant Pilots." *The Washington Post*, August 22, 2005, p. B1.

⁹⁹ Aircraft Owners and Pilots Association. *Congressional Bill Threatens GA With Expensive Security Mandates*. Frederick, MD (July 22, 2005).